



Object-store

REST API reference

NetApp

February 07, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi-9171/manage_s3_buckets.html on February 07, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Object-store	1
Manage S3 buckets	1
Manage S3 buckets	1
Retrieve all S3 buckets for all SVMs	19
Create the S3 bucket configuration for an SVM	53
Delete the S3 bucket configuration for an SVM	83
Retrieve the S3 bucket configuration for an SVM	87
Update the S3 bucket configuration for an SVM	111
Delete the S3 server configuration for an SVM	189
Retrieve the S3 server configuration for an SVM	193
Update the S3 server configuration for an SVM	226
Manage S3 service bucket configuration	252
Manage S3 service bucket configuration	252
Retrieve the S3 bucket configurations for an SVM	275
Create an S3 bucket configuration for an SVM	308
Manage S3 bucket lifecycle management rules	366
Manage S3 bucket lifecycle management rules	366
Retrieve S3 lifecycle rules for a bucket	369
Create the S3 bucket lifecycle rule configuration	379
Manage S3 bucket snapshots	400
Manage S3 bucket snapshots	400
Retrieve a collection of S3 bucket snapshots	406
Create an S3 bucket snapshot	412
Delete an S3 bucket snapshot	418
Retrieve details of a specific S3 bucket snapshot	420
Manage S3 service group configuration	425
Manage S3 service group configuration	425
Retrieve an S3 group configuration	429
Create an S3 group configuration	436
Delete an S3 group configuration for an SVM	443
Retrieve an S3 group configuration for an SVM	445
Update an S3 group configuration for an SVM	450
Retrieve S3 protocol historical performance metrics	456
Manage S3 service policies	464
Manage S3 service policies	464
Retrieve the S3 policies in an SVM configuration	470
Create an S3 policy configuration	480
Manage S3 service users	498
Manage S3 service users	498
Retrieve the SVM configuration for an S3 user	510
Create an S3 user configuration	517
Delete an S3 user configuration	524
Retrieve the S3 user configuration for an SVM	526

Update an S3 user configuration	531
---	-----

Object-store

Manage S3 buckets

Manage S3 buckets

Overview

An S3 bucket is a container of objects. Each bucket defines an object namespace. S3 server requests specify objects using a bucket-name and object-name pair. An object consists of data, along with optional metadata and access controls, that is accessible using a name. An object resides within a bucket. There can be more than one bucket in an S3 server. Buckets that are created for the server are associated with an S3 user that is created on the S3 server.

Examples

Retrieving all fields for all S3 buckets of a cluster

```
# The API:
/api/protocols/s3/buckets

# The call:
curl -X GET "https://<mgmt-
ip>/api/protocols/s3/buckets?fields=*&return_records=true" -H "accept:
application/json"

# The response:
{
  "records": [
    {
      "svm": {
        "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
        "name": "vs1"
      },
      "uuid": "527812ab-7c6d-11e9-97e8-0050568ea123",
      "name": "bucket-2",
      "volume": {
        "name": "fg_oss_1558514455",
        "uuid": "51276f5f-7c6d-11e9-97e8-0050568ea123"
      },
      "size": 209715200,
      "logical_used_size": 157286400,
      "encryption": {
        "enabled": false
      },
      "comment": "S3 bucket.",
      "qos_policy": {
```

```

    "min_throughput_iops": 0,
    "min_throughput_mbps": 0,
    "max_throughput_iops": 1000,
    "max_throughput_mbps": 0,
    "uuid": "39ac471f-ff35-11e9-b0f9-005056a7ab52",
    "name": "vs0_auto_gen_policy_39a9522f_ff35_11e9_b0f9_005056a7ab52"
  },
  "snapshot-policy": {
    "name": "default-1weekly",
    "uuid": "f9c5f090-4ac8-11ef-ba24-005056a7ceb6"
  },
},
{
  "svm": {
    "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
    "name": "vs1"
  },
  "uuid": "a8234aec-7e06-11e9-97e8-0050568ea123",
  "name": "bucket-1",
  "volume": {
    "name": "fg_oss_1558690256",
    "uuid": "a36a1ea7-7e06-11e9-97e8-0050568ea123"
  },
  "size": 1677721600,
  "logical_used_size": 0,
  "encryption": {
    "enabled": false
  },
  "comment": "bucket2",
  "qos_policy": {
    "min_throughput_iops": 0,
    "min_throughput_mbps": 0,
    "max_throughput_iops": 1000,
    "max_throughput_mbps": 0,
    "uuid": "39ac471f-ff35-11e9-b0f9-005056a7ab52",
    "name": "vs0_auto_gen_policy_39a9522f_ff35_11e9_b0f9_005056a7ab52"
  }
},
{
  "svm": {
    "uuid": "ee30eb2d-7ae1-11e9-8abe-0050568ea123",
    "name": "vs2"
  },
  "uuid": "19283b75-7ae2-11e9-8abe-0050568ea123",
  "name": "bucket-3",
  "volume": {

```

```

    "name": "fg_oss_1558690257",
    "uuid": "a46a1ea7-7e06-11e9-97e8-0050568ea123"
  },
  "size": 1677721600,
  "logical_used_size": 1075838976,
  "encryption": {
    "enabled": false
  },
  "comment": "bucket3",
  "qos_policy": {
    "min_throughput_iops": 0,
    "min_throughput_mbps": 0,
    "max_throughput_iops": 1000,
    "max_throughput_mbps": 0,
    "uuid": "39ac471f-ff35-11e9-b0f9-005056a7ab52",
    "name": "vs0_auto_gen_policy_39a9522f_ff35_11e9_b0f9_005056a7ab52"
  },
  "policy": {
    "statements": [
      {
        "effect": "allow",
        "actions": [
          "*"
        ],
        "principals": [
          "Alice"
        ],
        "resources": [
          "bucket-3",
          "bucket-3/*"
        ],
        "sid": "fullAccessForAliceToBucket",
        "conditions": [
          {
            "operator": "ip_address",
            "source_ips": [
              "1.1.1.1/10"
            ]
          }
        ]
      }
    ]
  },
  "cors": {
    "rules": [
      {

```

```

        "id": "string",
        "allowed_origins": [
            "http://www.example.com"
        ],
        "allowed_methods": [
            "PUT",
            "DELETE"
        ],
        "allowed_headers": [
            "x-amz-request-id"
        ],
        "expose_headers": [
            "http://www.example.com"
        ],
        "max_age_seconds": 1024
    }
]
}
},
"num_records": 3
}

```

Retrieving all S3 buckets of a cluster ordered by size

```
# The API:
/api/protocols/s3/buckets

# The call:
curl -X GET "https://<mgmt-
ip>/api/protocols/s3/buckets?return_records=true&order_by=size" -H
"accept: application/json"

# The response:
{
  "records": [
    {
      "svm": {
        "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
        "name": "vs1"
      },
      "uuid": "754389d0-7e13-11e9-bfdc-0050568ea123",
      "name": "bb1",
      "size": 838860800
    },
    {
      "svm": {
        "uuid": "ee30eb2d-7ae1-11e9-8abe-0050568ea123",
        "name": "vs2"
      },
      "uuid": "19283b75-7ae2-11e9-8abe-0050568ea123",
      "name": "bb2",
      "size": 838860800
    },
    {
      "svm": {
        "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
        "name": "vs1"
      },
      "uuid": "a8234aec-7e06-11e9-97e8-0050568ea123",
      "name": "bucket-1",
      "size": 1677721600
    }
  ],
  "num_records": 3
}
```

Retrieving all S3 buckets of a cluster with name "bb2"


```

# The API:
/api/protocols/s3/buckets

# The call:
curl -X GET "https://<mgmt-
ip>/api/protocols/s3/buckets?name=bb2&return_records=true" -H "accept:
application/json"

# The response:
{
  "records": [
    {
      "svm": {
        "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
        "name": "vs1"
      },
      "uuid": "087d940e-7e15-11e9-bfdc-0050568ea123",
      "name": "bb2"
    },
    {
      "svm": {
        "uuid": "ee30eb2d-7ae1-11e9-8abe-0050568ea123",
        "name": "vs2"
      },
      "uuid": "19283b75-7ae2-11e9-8abe-0050568ea123",
      "name": "bb2"
    }
  ],
  "num_records": 2
}

```

Retrieving the specified bucket associated with an SVM

```
# The API:
/api/protocols/s3/buckets/{svm.uuid}/{uuid}

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/s3/buckets/12f3ba4c-7ae0-11e9-8c06-0050568ea123/527812ab-7c6d-11e9-97e8-0050568ea123" -H "accept: application/json"

# The response:
{
  "svm": {
    "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
    "name": "vs1"
  },
  "uuid": "527812ab-7c6d-11e9-97e8-0050568ea123",
  "name": "bucket-2",
  "volume": {
    "name": "fg_oss_1558514455",
    "uuid": "51276f5f-7c6d-11e9-97e8-0050568ea123"
  },
  "size": 209715200,
  "logical_used_size": 157286400,
  "encryption": {
    "enabled": false
  },
  "comment": "S3 bucket.",
  "qos_policy": {
    "min_throughput_iops": 0,
    "min_throughput_mbps": 0,
    "max_throughput_iops": 1000,
    "max_throughput_mbps": 0,
    "uuid": "39ac471f-ff35-11e9-b0f9-005056a7ab52",
    "name": "vs0_auto_gen_policy_39a9522f_ff35_11e9_b0f9_005056a7ab52"
  }
}
```

Creating an S3 bucket for an SVM

```

# The API:
/api/protocols/s3/buckets

# The call:

curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/buckets?return_timeout=0&return_records=true" -H
"accept: application/json" -H "Content-Type: application/json" -d "{
  \"aggregates\": [ { \"name\": \"aggr5\", \"uuid\": \"12f3ba4c-7ae0-11e9-
8c06-0050568ea123\" } ], \"comment\": \"S3 bucket.\",
  \"constituents_per_aggregate\": 4, \"name\": \"bucket-3\", \"svm\": {
  \"name\": \"vs1\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-
005056bbbec1/?name=bucket-3
Content-Length: 353
Content-Type: application/json
{
  "num_records": 1,
  "records": [
    {
      "name": "bucket-3",
      "comment": "S3 bucket."
    }
  ],
  "job": {
    "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
      }
    }
  }
}

```

Creating an S3 bucket along with QoS policy for an SVM

```
# The API:
/api/protocols/s3/buckets

# The call:
curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/buckets?return_timeout=0&return_records=true" -H
"accept: application/json" -H "Content-Type: application/json" -d "{
\"comment\": \"S3 bucket.\", \"name\": \"bucket-3\", \"svm\": { \"name\":
\"vs1\" }, \"qos_policy\": { \"min_throughput_iops\": 0,
\"min_throughput_mbps\": 0, \"max_throughput_iops\": 1000000,
\"max_throughput_mbps\": 900000, \"uuid\": \"02d07a93-6177-11ea-b241-
000c293feac8\", \"name\":
\"vs0_auto_gen_policy_02cfa02a_6177_11ea_b241_000c293feac8\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-
005056bbbec1/?name=bucket-3
Content-Length: 353
Content-Type: application/json
{
  "num_records": 1,
  "records": [
    {
      "name": "bucket-3",
      "comment": "S3 bucket."
    }
  ],
  "job": {
    "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
      }
    }
  }
}
```

Creating an S3 bucket along with policies and conditions for an SVM

```
# The API:
/api/protocols/s3/buckets

# The call:

curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/buckets?return_timeout=0&return_records=true" -H
"accept: application/json" -H "Content-Type: application/json" -d "{
\"aggregates\": [ { \"name\": \"aggr5\", \"uuid\": \"12f3ba4c-7ae0-11e9-
8c06-0050568ea123\" } ], \"comment\": \"S3 bucket.\",
\"constituents_per_aggregate\": 4, \"name\": \"bucket-3\", \"policy\": {
\"statements\": [ { \"actions\": [ \"GetObject\" ], \"conditions\": [ {
\"operator\": \"ip_address\", \"source_ips\": [ \"1.1.1.1/23\",
\"1.2.2.2/20\" ] } ], \"effect\": \"allow\", \"resources\": [ \"bucket-
3/policies/examples/*\" ], \"sid\": \"AccessToGetObjectForAllUsersofSVM\"
}, { \"actions\": [ \"*Object\" ], \"effect\": \"deny\", \"principals\": [
\"mike\" ], \"resources\": [ \"bucket-3/policy-docs/*\", \"bucket-
3/confidential-*\" ], \"sid\": \"DenyAccessToObjectForMike\" }, {
\"actions\": [ \"GetObject\" ], \"effect\": \"allow\", \"principals\": [
\"*\" ], \"resources\": [ \"bucket-3/readme\" ], \"sid\":
\"AnonymousAccessToGetObjectForUsers\" } ] }, \"svm\": { \"uuid\":
\"259b4e46-2d33-11ea-9145-005056bbbec1\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-
005056bbbec1/?name=bucket-3
Content-Length: 353
Content-Type: application/json
{
  "num_records": 1,
  "records": [
    {
      "name": "bucket-3",
      "comment": "S3 bucket."
    }
  ],
  "job": {
```

```
"uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
"_links": {
  "self": {
    "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
  }
}
}
```

Creating an S3 bucket and CORS rules for an SVM

```
# The API:
/api/protocols/s3/buckets

# The call:

curl -X POST "https://<mgmt-
ip>/api/protocols/s3/buckets?return_timeout=0&return_records=true" -H
"accept: application/json" -H "Content-Type: application/json" -d "{
  \"aggregates\": [ { \"name\": \"aggr5\", \"uuid\": \"12f3ba4c-7ae0-11e9-
8c06-0050568ea123\" } ], \"comment\": \"S3 bucket.\",
  \"constituents_per_aggregate\": 4, \"name\": \"bucket-3\", \"cors\": {
  \"rules\": [{ \"allowed_headers\": [ \"x-amz-request-id\" ],
  \"allowed_methods\": [ \"PUT\", \"DELETE\" ], \"allowed_origins\": [
  \"http://www.example.com\" ], \"expose_headers\": [
  \"http://www.example.com\" ], \"id\": \"id1\", \"max_age_seconds\": 1024
  ]}], \"svm\": { \"uuid\": \"259b4e46-2d33-11ea-9145-005056bbbec1\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-
005056bbbec1/?name=bucket-3
Content-Length: 353
Content-Type: application/json
{
  "num_records": 1,
  "records": [
    {
      "name": "bucket-3",
      "comment": "S3 bucket."
    }
  ],
  "job": {
    "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
      }
    }
  }
}
```

Creating an S3 bucket along with a bucket lifecycle management rule for an SVM

```
# The API:
/api/protocols/s3/buckets

# The call:

curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/buckets?return_timeout=0&return_records=true" -H
"accept: application/json" -H "Content-Type: application/json" -d "{
  \"aggregates\": [ { \"name\": \"aggr5\", \"uuid\": \"12f3ba4c-7ae0-11e9-
8c06-0050568ea123\" } ], \"comment\": \"S3 bucket.\",
  \"constituents_per_aggregate\": 4, \"name\": \"bucket-4\",
  \"lifecycle_management\": { \"rules\": [ { \"name\": \"rule1\",
  \"expiration\": { \"object_age_days\" : \"1000\" } },
  \"abort_incomplete_multipart_upload\" : { \"after_initiation_days\" : 200
}, \"object_filter\": { \"prefix\" : \"obj1*/\" , \"size_greater_than\" :
  \"1000\" } } ], { \"name\": \"rule2\", \"object_filter\": {
  \"size_greater_than\" : \"50\" } }, \"expiration\": { \"object_age_days\" :
  \"5000\" } } ] } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 18 April 2022 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-
005056bbbec1/?name=bucket-4
Content-Length: 353
Content-Type: application/json
{
  "num_records": 1,
  "records": [
    {
      "name": "bucket-4",
      "comment": "S3 bucket."
    }
  ],
  "job": {
    "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
```



```

    }
  }
}
}

```

Creating an S3 bucket with a snapshot-policy

```

# The API:
/api/protocols/s3/buckets

# The call:
curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/buckets?return_records=true" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"comment\":
\"S3 snapshot policy bucket.\", \"snapshot_policy\": { \"name\":
\"default-1weekly\", \"uuid\": \"f9c5f090-4ac8-11ef-ba24-005056a7ceb6\" },
\"name\": \"bucket-7\", \"svm.uuid\": \"8c38f10b-4871-11ef-aab5-
005056a7ceb6\" }"

# The response:
HTTP/1.1 202 Accepted
Date: Thu, 25 Jul 2024 17:16:15 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/8c38f10b-4871-11ef-aab5-
005056a7ceb6/buckets/9f21f404-4aa4-11ef-ba24-005056a7ceb6
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "99978136-4aa9-11ef-ba24-005056a7ceb6",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/99978136-4aa9-11ef-ba24-005056a7ceb6"
      }
    }
  }
}

```

Updating an S3 bucket for an SVM

```

# The API:
/api/protocols/s3/buckets/{svm.uuid}/{uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-005056bbbec1/376a2efd-2d4d-11ea-9c30-005056bb883a?return_records=true" -H "accept: application/json?return_records=true" -H "Content-Type: application/json" -d "{ \"comment\": \"Bucket modified.\", \"size\": 11111111111, \"qos_policy\": { \"min_throughput_iops\": 0, \"min_throughput_mbps\": 0, \"max_throughput_iops\": 1000000, \"max_throughput_mbps\": 900000, \"uuid\": \"02d07a93-6177-11ea-b241-000c293feac8\", \"name\": \"vs0_auto_gen_policy_02cfa02a_6177_11ea_b241_000c293feac8\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "9beafabb-7e17-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/9beafabb-7e17-11e9-bfdc-0050568ea123"
      }
    }
  }
}

```

Updating an S3 bucket policy for an SVM

```

# The API:
/api/protocols/s3/buckets/{svm.uuid}/{uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-005056bbbec1/376a2efd-2d4d-11ea-9c30-005056bb883a?return_records=true" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"policy\": { \"statements\": [ { \"actions\": [ \"*\"] , \"conditions\": [ { \"operator\": \"ip_address\", \"source_ips\": [ \"1.1.1.5/23\" ] } ] , \"effect\": \"allow\", \"resources\": [ \"*\"] , \"sid\": \"fullAccessForAllPrincipalsToBucket\" } ] } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "9beafabb-7e17-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/9beafabb-7e17-11e9-bfdc-0050568ea123"
      }
    }
  }
}

```

Updating an S3 bucket CORS configuration for an SVM

```
# The API:
/api/protocols/s3/buckets/{svm.uuid}/{uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-005056bbbec1/376a2efd-2d4d-11ea-9c30-005056bb883a?return_records=true" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"cors\": { \"rules\": [{ \"allowed_headers\": [ \"x-amz-request-id\" ], \"allowed_methods\": [ \"PUT\", \"DELETE\" ], \"allowed_origins\": [ \"http://www.example.com\" ], \"expose_headers\": [ \"http://www.example.com\" ], \"id\": \"id1\", \"max_age_seconds\": 1024 } ] } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "9beafabb-7e17-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/9beafabb-7e17-11e9-bfdc-0050568ea123"
      }
    }
  }
}
```

Updating the snapshot-policy for an S3 bucket for an SVM

```
# The API:
/api/protocols/s3/buckets/{svm.uuid}/{uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/buckets/8c38f10b-4871-11ef-aab5-005056a7ceb6/eec0d90e-4934-11ef-947d-005056a7ceb6" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"snapshot_policy\": { \"name\": \"default-1weekly\", \"uuid\": \"f9c5f090-4ac8-11ef-ba24-005056a7ceb6\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Thu, 25 Jul 2024 17:26:17 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "003a4cad-4aab-11ef-ba24-005056a7ceb6",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/003a4cad-4aab-11ef-ba24-005056a7ceb6"
      }
    }
  }
}
```

Deleting an S3 bucket for a specified SVM

```
# The API:
/api/protocols/s3/buckets/{svm.uuid}/{uuid}

# The call:
curl -iku admin:<password> -X DELETE "https://<mgmt-
ip>/api/protocols/s3/buckets/259b4e46-2d33-11ea-9145-
005056bbbec1/98528221-2d52-11ea-892e-005056bbbec1?return_records=true" -H
"accept: application/json"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:40:17 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "b3af4a54-7e18-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/b3af4a54-7e18-11e9-bfdc-0050568ea123"
      }
    }
  }
}
```

Retrieve all S3 buckets for all SVMs

GET /protocols/s3/buckets

Introduced In: 9.7

Retrieves all S3 buckets for all SVMs. Note that in order to retrieve S3 bucket policy conditions, the 'fields' option should be set to '**'.

Related ONTAP commands

- vserver object-store-server bucket show
- vserver object-store-server bucket policy statement show
- vserver object-store-server bucket policy-statement-condition show
- vserver object-store-server bucket lifecycle-management-rule show
- vserver object-store-server bucket cors-rule show

Learn more

- [DOC /protocols/s3/buckets](#)

Parameters

Name	Type	In	Required	Description
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
lifecycle_management.rules.uuid	string	query	False	Filter by lifecycle_management.rules.uuid <ul style="list-style-type: none">• Introduced in: 9.14
lifecycle_management.rules.name	string	query	False	Filter by lifecycle_management.rules.name <ul style="list-style-type: none">• Introduced in: 9.13• maxLength: 256• minLength: 0
lifecycle_management.rules.bucket_name	string	query	False	Filter by lifecycle_management.rules.bucket_name <ul style="list-style-type: none">• Introduced in: 9.14• maxLength: 63• minLength: 3
lifecycle_management.rules.non_current_version_expiration.new_non_current_versions	integer	query	False	Filter by lifecycle_management.rules.non_current_version_expiration.new_non_current_versions <ul style="list-style-type: none">• Introduced in: 9.13

Name	Type	In	Required	Description
lifecycle_management.rules.non_current_version_expiration.non_current_days	integer	query	False	Filter by lifecycle_management.rules.non_current_version_expiration.non_current_days • Introduced in: 9.13
lifecycle_management.rules.expiration.object_age_days	integer	query	False	Filter by lifecycle_management.rules.expiration.object_age_days • Introduced in: 9.13
lifecycle_management.rules.expiration.expired_object_delete_marker	boolean	query	False	Filter by lifecycle_management.rules.expiration.expired_object_delete_marker • Introduced in: 9.13
lifecycle_management.rules.expiration.object_expiry_date	string	query	False	Filter by lifecycle_management.rules.expiration.object_expiry_date • Introduced in: 9.13
lifecycle_management.rules.object_filter.tags	string	query	False	Filter by lifecycle_management.rules.object_filter.tags • Introduced in: 9.13
lifecycle_management.rules.object_filter.prefix	string	query	False	Filter by lifecycle_management.rules.object_filter.prefix • Introduced in: 9.13

Name	Type	In	Required	Description
lifecycle_management.rules.object_filter.size_greater_than	integer	query	False	Filter by lifecycle_management.rules.object_filter.size_greater_than • Introduced in: 9.13
lifecycle_management.rules.object_filter.size_less_than	integer	query	False	Filter by lifecycle_management.rules.object_filter.size_less_than • Introduced in: 9.13
lifecycle_management.rules.enabled	boolean	query	False	Filter by lifecycle_management.rules.enabled • Introduced in: 9.13
lifecycle_management.rules.abort_incomplete_multipart_upload.after_initiation_days	integer	query	False	Filter by lifecycle_management.rules.abort_incomplete_multipart_upload.after_initiation_days • Introduced in: 9.13
lifecycle_management.rules.svm.name	string	query	False	Filter by lifecycle_management.rules.svm.name • Introduced in: 9.14
lifecycle_management.rules.svm.uuid	string	query	False	Filter by lifecycle_management.rules.svm.uuid • Introduced in: 9.14

Name	Type	In	Required	Description
comment	string	query	False	Filter by comment <ul style="list-style-type: none"> • maxLength: 256 • minLength: 0
encryption.enabled	boolean	query	False	Filter by encryption.enabled
policy.statements.resources	string	query	False	Filter by policy.statements.resources <ul style="list-style-type: none"> • Introduced in: 9.8
policy.statements.actions	string	query	False	Filter by policy.statements.actions <ul style="list-style-type: none"> • Introduced in: 9.8
policy.statements.effect	string	query	False	Filter by policy.statements.effect <ul style="list-style-type: none"> • Introduced in: 9.8
policy.statements.conditions.usernames	string	query	False	Filter by policy.statements.conditions.usernames <ul style="list-style-type: none"> • Introduced in: 9.8
policy.statements.conditions.source_ips	string	query	False	Filter by policy.statements.conditions.source_ips <ul style="list-style-type: none"> • Introduced in: 9.8
policy.statements.conditions.max_keys	integer	query	False	Filter by policy.statements.conditions.max_keys <ul style="list-style-type: none"> • Introduced in: 9.8

Name	Type	In	Required	Description
policy.statements.conditions.delimiters	string	query	False	Filter by policy.statements.conditions.delimiters <ul style="list-style-type: none"> Introduced in: 9.8
policy.statements.conditions.operator	string	query	False	Filter by policy.statements.conditions.operator <ul style="list-style-type: none"> Introduced in: 9.8
policy.statements.conditions.prefixes	string	query	False	Filter by policy.statements.conditions.prefixes <ul style="list-style-type: none"> Introduced in: 9.8
policy.statements.principals	string	query	False	Filter by policy.statements.principals <ul style="list-style-type: none"> Introduced in: 9.8
policy.statements.sid	string	query	False	Filter by policy.statements.sid <ul style="list-style-type: none"> Introduced in: 9.8 maxLength: 256 minLength: 0
qos_policy.min_throughput_mbps	integer	query	False	Filter by qos_policy.min_throughput_mbps <ul style="list-style-type: none"> Introduced in: 9.8 Max value: 4194303 Min value: 0

Name	Type	In	Required	Description
qos_policy.max_throughput_mbps	integer	query	False	Filter by qos_policy.max_throughput_mbps <ul style="list-style-type: none"> • Introduced in: 9.8 • Max value: 4194303 • Min value: 0
qos_policy.name	string	query	False	Filter by qos_policy.name <ul style="list-style-type: none"> • Introduced in: 9.8
qos_policy.uuid	string	query	False	Filter by qos_policy.uuid <ul style="list-style-type: none"> • Introduced in: 9.8
qos_policy.max_throughput	string	query	False	Filter by qos_policy.max_throughput <ul style="list-style-type: none"> • Introduced in: 9.17
qos_policy.max_throughput_iops	integer	query	False	Filter by qos_policy.max_throughput_iops <ul style="list-style-type: none"> • Introduced in: 9.8 • Max value: 2147483647 • Min value: 0

Name	Type	In	Required	Description
qos_policy.min_throughput_iops	integer	query	False	Filter by qos_policy.min_throughput_iops <ul style="list-style-type: none"> • Introduced in: 9.8 • Max value: 2147483647 • Min value: 0
qos_policy.min_throughput	string	query	False	Filter by qos_policy.min_throughput <ul style="list-style-type: none"> • Introduced in: 9.17
role	string	query	False	Filter by role <ul style="list-style-type: none"> • Introduced in: 9.10
size	integer	query	False	Filter by size <ul style="list-style-type: none"> • Max value: 62672162783232000 • Min value: 199229440
is_nas_path_mutable	boolean	query	False	Filter by is_nas_path_mutable <ul style="list-style-type: none"> • Introduced in: 9.17
uuid	string	query	False	Filter by uuid
logical_used_size	integer	query	False	Filter by logical_used_size
allowed	boolean	query	False	Filter by allowed <ul style="list-style-type: none"> • Introduced in: 9.12

Name	Type	In	Required	Description
versioning_state	string	query	False	Filter by versioning_state <ul style="list-style-type: none"> Introduced in: 9.11
cors.rules.expose_headers	string	query	False	Filter by cors.rules.expose_headers <ul style="list-style-type: none"> Introduced in: 9.16
cors.rules.max_age_seconds	integer	query	False	Filter by cors.rules.max_age_seconds <ul style="list-style-type: none"> Introduced in: 9.16
cors.rules.allowed_origins	string	query	False	Filter by cors.rules.allowed_origins <ul style="list-style-type: none"> Introduced in: 9.16
cors.rules.allowed_methods	string	query	False	Filter by cors.rules.allowed_methods <ul style="list-style-type: none"> Introduced in: 9.16
cors.rules.allowed_headers	string	query	False	Filter by cors.rules.allowed_headers <ul style="list-style-type: none"> Introduced in: 9.16
cors.rules.id	string	query	False	Filter by cors.rules.id <ul style="list-style-type: none"> Introduced in: 9.16 maxLength: 256 minLength: 0

Name	Type	In	Required	Description
nas_path	string	query	False	Filter by nas_path • Introduced in: 9.12
retention.mode	string	query	False	Filter by retention.mode • Introduced in: 9.14
retention.default_period	string	query	False	Filter by retention.default_period • Introduced in: 9.14
snapshot_policy.uuid	string	query	False	Filter by snapshot_policy.uuid • Introduced in: 9.16
snapshot_policy.name	string	query	False	Filter by snapshot_policy.name • Introduced in: 9.16
audit_event_selector.permission	string	query	False	Filter by audit_event_selector.permission • Introduced in: 9.10
audit_event_selector.access	string	query	False	Filter by audit_event_selector.access • Introduced in: 9.10

Name	Type	In	Required	Description
protection_status.is_protected	boolean	query	False	Filter by protection_status.is_protected • Introduced in: 9.10
protection_status.destination.is_ontap	boolean	query	False	Filter by protection_status.destination.is_ontap • Introduced in: 9.10
protection_status.destination.is_external_cloud	boolean	query	False	Filter by protection_status.destination.is_external_cloud • Introduced in: 9.12
protection_status.destination.is_cloud	boolean	query	False	Filter by protection_status.destination.is_cloud • Introduced in: 9.10
type	string	query	False	Filter by type • Introduced in: 9.12
volume.uuid	string	query	False	Filter by volume.uuid
volume.name	string	query	False	Filter by volume.name
is_consistent_etag	boolean	query	False	Filter by is_consistent_etag • Introduced in: 9.17

Name	Type	In	Required	Description
name	string	query	False	Filter by name <ul style="list-style-type: none"> • maxLength: 63 • minLength: 3
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. <ul style="list-style-type: none"> • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. <ul style="list-style-type: none"> • Max value: 120 • Min value: 0 • Default value: 15
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

Status: 200, Ok

Name	Type	Description
_links	collection_links	
num_records	integer	Number of records
records	array[s3_bucket]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "audit_event_selector": {
        "access": "string",
        "permission": "string"
      },
      "comment": "S3 bucket.",
      "cors": {
        "rules": [
          {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "allowed_headers": [
              "x-amz-request-id"
            ],
            "allowed_methods": [
              "PUT",
              "DELETE"
            ],
            "allowed_origins": [
              "http://www.example.com"
            ],
            "expose_headers": [
              "x-amz-date"
            ],
            "id": "string",
            "max_age_seconds": 1024
          }
        ]
      },
      "lifecycle_management": {
```

```

"rules": [
  {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "abort_incomplete_multipart_upload": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    },
    "bucket_name": "bucket1",
    "expiration": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    },
    "object_age_days": 100,
    "object_expiry_date": "2039-09-22 20:00:00 -0400"
  },
  "name": "string",
  "non_current_version_expiration": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "object_filter": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "prefix": "/logs",
  "size_greater_than": 10240,
  "size_less_than": 10485760,
  "tags": [
    "project1=projA",
    "project2=projB"
  ]
},

```

```

    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055"
  ]
},
"logical_used_size": 0,
"name": "bucket1",
"nas_path": "/",
"policy": {
  "statements": [
    {
      "actions": [
        "GetObject",
        "PutObject",
        "DeleteObject",
        "ListBucket"
      ],
      "conditions": [
        {
          "delimiters": [
            "/"
          ],
          "max_keys": [
            1000
          ],
          "operator": "ip_address",
          "prefixes": [
            "pref"
          ],
          "source_ips": [
            "1.1.1.1",
            "1.2.2.0/24"
          ],
          "usernames": [
            "user1"
          ]
        }
      ]
    }
  ],

```

```

        "effect": "allow",
        "principals": [
            "user1",
            "group/grp1",
            "nasgroup/group1"
        ],
        "resources": [
            "bucket1",
            "bucket1/*"
        ],
        "sid": "FullAccessToUser1"
    }
]
},
"qos_policy": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    },
    "max_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
    ],
    "max_throughput_iops": 10000,
    "max_throughput_mbps": 500,
    "min_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
    ],
    "min_throughput_iops": 2000,
    "min_throughput_mbps": 500,
    "name": "performance",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"retention": {

```

```

    "default_period": "P10Y",
    "mode": "governance"
  },
  "role": "string",
  "size": 1677721600,
  "snapshot_policy": {
    "name": "default-1weekly",
    "uuid": "3675af31-431c-12fa-114a-20675afebc12"
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "type": "s3",
  "use_mirrored_aggregates": true,
  "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055",
  "versioning_state": "enabled",
  "volume": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "volume1",
    "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
  }
}
]
}

```

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

collection_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

aggregates

Aggregate

Name	Type	Description
_links	_links	
name	string	
uuid	string	

audit_event_selector

Audit event selector allows you to specify access and permission types to audit.

Name	Type	Description
access	string	Specifies read and write access types.
permission	string	Specifies allow and deny permission types.

rules

Information about the CORS rule of an S3 bucket.

Name	Type	Description
_links	_links	

Name	Type	Description
allowed_headers	array[string]	An array of HTTP headers allowed in the cross-origin requests.
allowed_methods	array[string]	An array of HTTP methods allowed in the cross-origin requests.
allowed_origins	array[string]	List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.
expose_headers	array[string]	List of extra headers sent in the response that customers can access from their applications.
id	string	Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
max_age_seconds	integer	The time in seconds for your browser to cache the preflight response for the specified resource.

cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
rules	array[rules]	Specifies an object store bucket CORS rule.

encryption

Name	Type	Description
enabled	boolean	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be specified in a POST method.

abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
_links	_links	
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
new_non_current_versions	integer	Number of latest non-current versions to be retained.
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
_links	_links	

Name	Type	Description
prefix	string	A prefix that is matched against object-names within a bucket.
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

rules

Information about the lifecycle management rule of a bucket.

Name	Type	Description
_links	_links	
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
bucket_name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
name	string	Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
object_filter	object_filter	Specifies a way to filter objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

Name	Type	Description
rules	array[rules]	Specifies an object store lifecycle management policy.

s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

Name	Type	Description
delimiters	array[string]	An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.
max_keys	array[integer]	An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.
operator	string	Condition operator that is applied to the specified condition key.
prefixes	array[string]	An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.
source_ips	array[string]	An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.
usernames	array[string]	An array of usernames that a current user in the context is evaluated against using the condition operators.

s3_bucket_policy_statement

Specifies information about a single access permission.

Name	Type	Description
actions	array[string]	
conditions	array[s3_bucket_policy_condition]	Specifies bucket policy conditions.

Name	Type	Description
effect	string	Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
principals	array[string]	
resources	array[string]	
sid	string	Specifies the statement identifier used to differentiate between statements. The sid length can range from 1 to 256 characters and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

Name	Type	Description
statements	array[s3_bucket_policy_statement]	Specifies bucket access policy statement.

destination

Name	Type	Description
is_cloud	boolean	Specifies whether a bucket is protected within the Cloud. This field cannot be specified using a POST method.
is_external_cloud	boolean	Specifies whether a bucket is protected on external Cloud providers. This field cannot be specified using a POST method.

Name	Type	Description
is_ontap	boolean	<p>Specifies whether a bucket is protected within ONTAP. This field cannot be specified using a POST method.</p> <ul style="list-style-type: none"> • Default value: • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

protection_status

Specifies attributes of bucket protection.

Name	Type	Description
destination	destination	
is_protected	boolean	<p>Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be specified using a POST method.</p> <ul style="list-style-type: none"> • Default value: • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

Name	Type	Description
_links	_links	

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

retention

Specifies the retention mode and default retention period configured on the bucket.

Name	Type	Description
default_period	string	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.</num></num>
mode	string	The lock mode of the bucket. compliance ‐ A SnapLock Compliance (SLC) bucket provides the highest level of WORM protection and an administrator cannot destroy a compliance bucket if it contains unexpired WORM objects. governance ‐ An administrator can delete a Governance bucket. no_lock ‐ Indicates the bucket does not support object locking.

snapshot_policy

Specifies the bucket snapshot policy.

Name	Type	Description
name	string	Specifies the name of the snapshot policy.
uuid	string	Specifies the unique identifier of the snapshot policy.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted.

Name	Type	Description
_links	_links	
name	string	The name of the volume. This field cannot be specified in a PATCH method.
uuid	string	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move. <ul style="list-style-type: none">• example: 028baa66-41bd-11e9-81d5-00a0986138f7• Introduced in: 9.6• x-nullable: true

s3_bucket

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.

Name	Type	Description
audit_event_selector	audit_event_selector	Audit event selector allows you to specify access and permission types to audit.
comment	string	Can contain any additional information about the bucket being created or modified.
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
is_nas_path_mutable	boolean	Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.

Name	Type	Description
lifecycle_management	lifecycle_management	Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.
name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.

Name	Type	Description
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be specified using a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Specifies the bucket type. Valid values are "s3" and "nas".
uuid	string	Specifies the unique identifier of the bucket.

Name	Type	Description
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create the S3 bucket configuration for an SVM

POST /protocols/s3/buckets

Introduced In: 9.8

Creates the S3 bucket configuration of an SVM.

Important notes

- Each SVM can have one or more bucket configurations.
- Aggregate lists should be specified explicitly. If not specified, then the bucket is auto-provisioned as a FlexGroup volume.

- Constituents per aggregate specifies the number of components (or FlexVol volumes) per aggregate. Is specified only when an aggregate list is explicitly defined.
- An access policy can be created along with a bucket create. If creating an access policy fails, bucket configurations are saved and the access policy can be created using the PATCH endpoint.
- "qos_policy" can be specified if a bucket needs to be attached to a QoS group policy during creation time.
- "audit_event_selector" can be specified if a bucket needs to be specify access and permission type for auditing.
- A CORS configuration can be specified along with bucket creation.

Required properties

- `svm.uuid` or `svm.name` - Existing SVM in which to create the bucket configuration.
- `name` - Bucket name that is to be created.

Recommended optional properties

- `aggregates` - List of aggregates for the FlexGroup volume on which the bucket is hosted on.
- `constituents_per_aggregate` - Number of constituents per aggregate.
- `size` - Specifying the bucket size is recommended.
- `policy` - Specifying a policy enables users to perform operations on buckets; specifying the resource permissions is recommended.
- `qos_policy` - A QoS policy for buckets.
- `audit_event_selector` - Audit policy for buckets.
- `versioning_state` - Versioning state for buckets.
- `type` - Type of bucket.
- `nas_path` - NAS path to which the bucket corresponds to.
- `use_mirrored_aggregates` - Specifies whether mirrored aggregates are selected when provisioning a FlexGroup volume.
- `lifecycle_management` - Object store server lifecycle management policy.
- `retention.mode` - Object lock mode supported on the bucket.
- `retention.default_period` - Specifies the duration of default-retention applicable for objects on the object store bucket.
- `cors` - Specifying CORS rules enables the bucket to service the cross-origin requests.
- `snapshot_policy` - Snapshot policy for the bucket.
- `is_nas_path_mutable` - Specifies whether the NAS bucket mapping with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount.

Default property values

- `size` - 800MB
- `comment` - ""

- `aggregates` - No default value.
- `constituents_per_aggregate` - `4` , if an `aggregates` list is specified. Otherwise, no default value.
- `policy.statements.actions` - `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `ListBucketMultipartUploads`, `ListMultipartUploadParts`, `GetObjectTagging`, `PutObjectTagging`, `DeleteObjectTagging`, `GetBucketVersioning`, `PutBucketVersioning`.
- `policy.statements.principals` - all S3 users and groups in the SVM or the NAS groups.
- `policy.statements.resources` - all objects in the bucket.
- `policy.statements.conditions` - list of bucket policy conditions.
- `versioning_state` - `disabled`.
- `use_mirrored_aggregates` - *true* for a MetroCluster configuration and *false* for a non-MetroCluster configuration.
- `type` - `S3`
- `retention.mode` - `no_lock`

Related ONTAP commands

- `vserver object-store-server bucket create`
- `vserver object-store-server bucket policy statement create`
- `vserver object-store-server bucket lifecycle-management-rule create`
- `vserver object-store-server bucket cors-rule create`

Learn more

- [DOC /protocols/s3/buckets](#)

Parameters

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none"> • Default value: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	<p>The default is false. If set to true, the records are returned.</p> <ul style="list-style-type: none"> • Default value:

Request Body

Name	Type	Description
aggregates	array[aggregates]	A list of aggregates for FlexGroup volume constituents where the bucket is hosted. If this option is not specified, the bucket is auto-provisioned as a FlexGroup volume.
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.
audit_event_selector	audit_event_selector	Audit event selector allows you to specify access and permission types to audit.
comment	string	Can contain any additional information about the bucket being created or modified.
constituents_per_aggregate	integer	Specifies the number of constituents or FlexVol volumes per aggregate. A FlexGroup volume consisting of all such constituents across all specified aggregates is created. This option is used along with the aggregates option and cannot be used independently.
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
encryption	encryption	

Name	Type	Description
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
is_nas_path_mutable	boolean	Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.
lifecycle_management	lifecycle_management	Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.
name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.

Name	Type	Description
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps" . Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be specified using a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.

Name	Type	Description
storage_service_level	string	Specifies the storage service level of the FlexGroup volume on which the bucket should be created. Valid values are "value", "performance" or "extreme".
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Specifies the bucket type. Valid values are "s3" and "nas".
use_mirrored_aggregates	boolean	Specifies whether mirrored aggregates are selected when provisioning a FlexGroup. Only mirrored aggregates are used if this parameter is set to "true" and only unmirrored aggregates are used if this parameter is set to "false". The default value is "true" for a MetroCluster configuration and is "false" for a non-MetroCluster configuration.
uuid	string	Specifies the unique identifier of the bucket.
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted.

Example request

```
{
  "aggregates": [
    {
      "name": "aggr1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ],
  "audit_event_selector": {
    "access": "string",
    "permission": "string"
  },
  "comment": "S3 bucket.",
  "constituents_per_aggregate": 4,
  "cors": {
    "rules": [
      {
        "allowed_headers": [
          "x-amz-request-id"
        ],
        "allowed_methods": [
          "PUT",
          "DELETE"
        ],
        "allowed_origins": [
          "http://www.example.com"
        ],
        "expose_headers": [
          "x-amz-date"
        ],
        "id": "string",
        "max_age_seconds": 1024
      }
    ]
  },
  "lifecycle_management": {
    "rules": [
      {
        "bucket_name": "bucket1",
        "expiration": {
          "object_age_days": 100,
          "object_expiry_date": "2039-09-22 20:00:00 -0400"
        },
        "name": "string",
        "object_filter": {
```



```

        "prefix": "/logs",
        "size_greater_than": 10240,
        "size_less_than": 10485760,
        "tags": [
            "project1=projA",
            "project2=projB"
        ]
    },
    "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055"
}
]
},
"logical_used_size": 0,
"name": "bucket1",
"nas_path": "/",
"policy": {
    "statements": [
        {
            "actions": [
                "GetObject",
                "PutObject",
                "DeleteObject",
                "ListBucket"
            ],
            "conditions": [
                {
                    "delimiters": [
                        "/"
                    ],
                    "max_keys": [
                        1000
                    ],
                    "operator": "ip_address",
                    "prefixes": [
                        "pref"
                    ],
                    "source_ips": [
                        "1.1.1.1",
                        "1.2.2.0/24"
                    ],
                    "usernames": [
                        "user1"
                    ]
                }
            ]
        }
    ]
}

```

```

        ]
    }
],
"effect": "allow",
"principals": [
    "user1",
    "group/grp1",
    "nasgroup/group1"
],
"resources": [
    "bucket1",
    "bucket1/*"
],
"sid": "FullAccessToUser1"
}
]
},
"qos_policy": {
    "max_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
    ],
    "max_throughput_iops": 10000,
    "max_throughput_mbps": 500,
    "min_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
    ],
    "min_throughput_iops": 2000,
    "min_throughput_mbps": 500,
    "name": "performance",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"retention": {
    "default_period": "P10Y",
    "mode": "governance"
}

```

```

    },
    "role": "string",
    "size": 1677721600,
    "snapshot_policy": {
      "name": "default-1weekly",
      "uuid": "3675af31-431c-12fa-114a-20675afebc12"
    },
    "storage_service_level": "value",
    "svm": {
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "type": "s3",
    "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055",
    "versioning_state": "enabled",
    "volume": {
      "name": "volume1",
      "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
    }
  }
}

```

Response

Status: 202, Accepted

Name	Type	Description
job	job_link	

Example response

```

{
  "job": {
    "uuid": "string"
  }
}

```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Response

Status: 201, Created

Error

Status: Default

ONTAP Error Response Codes

Error code	Message
92405777	"Failed to create bucket "{bucket name}" for SVM "{svm.name}". Reason: {Reason of failure}.";
92405785	"Bucket name "{bucket name}" contains invalid characters or invalid character combinations. Valid characters for a bucket name are 0-9, a-z, ".", and "-". Invalid character combinations are "-.", "-.", and "..".";
92405786	"Bucket name "{bucket name}" is not valid. Bucket names must have between 3 and 63 characters. ";
92405811	"Failed to create bucket "{bucket name}" for SVM "{svm.name}". Wait a few minutes and try the operation again.";
92405812	"Failed to create the object store volume. Reason: {Reason for failure}.";
92405819	"Cannot provision an object store server volume for bucket "{bucket name}" in SVM "{svm.name}" on the following aggregates because they are SnapLock aggregates: {List of aggregates.name}.";
92405820	"Failed to check whether the aggregate "{aggregates.name}" is a FabricPool. Reason: {Reason for failure}.";
92405821	"Cannot provision an object store server volume for bucket "{bucket name}" in SVM "{svm.name}" on the following aggregates because they are FabricPool: {List of aggregates.name}.";
92405827	"Internal Error. Unable to generate object store volume name.";
92405857	"One or more aggregates must be specified if "constituents_per_aggregate" is specified.";
92405858	"Failed to "create" the "bucket" because the operation is only supported on data SVMs.";
92405859	"The specified "aggregates.uuid" "{aggregates.uuid}" does not exist.";

Error code	Message
92405860	"The specified "aggregates.name" "{aggregates.name}" and "aggregates.uuid" "{aggregates.uuid}" refer to different aggregates.";
92405861	"The specified SVM UUID or bucket UUID does not exist.";
92405863	"An error occurs when creating an access policy. The reason for failure is detailed in the error message.";
92405863	"Failed to create lifecycle management rules for bucket "s3bucket1". Reason: {Reason of failure}. ";
92405891	The resources specified in the access policy are not valid. Valid ways to specify a resource are *, <bucket-name>, <bucket-name>/.../.... Valid characters for a resource are 0-9, A-Z, a-z, _, +, comma, ;, :, =, ., &, @, ?, (,), single quote, *, !, - and \$.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

aggregates

Aggregate

Name	Type	Description
name	string	
uuid	string	

audit_event_selector

Audit event selector allows you to specify access and permission types to audit.

Name	Type	Description
access	string	Specifies read and write access types.
permission	string	Specifies allow and deny permission types.

rules

Information about the CORS rule of an S3 bucket.

Name	Type	Description
allowed_headers	array[string]	An array of HTTP headers allowed in the cross-origin requests.
allowed_methods	array[string]	An array of HTTP methods allowed in the cross-origin requests.
allowed_origins	array[string]	List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.

Name	Type	Description
expose_headers	array[string]	List of extra headers sent in the response that customers can access from their applications.
id	string	Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
max_age_seconds	integer	The time in seconds for your browser to cache the preflight response for the specified resource.

cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
rules	array[rules]	Specifies an object store bucket CORS rule.

encryption

Name	Type	Description
enabled	boolean	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be specified in a POST method.

abort_incomplete_multipart_upload

Specifies a way to perform `abort_incomplete_multipart_upload` action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
new_non_current_versions	integer	Number of latest non-current versions to be retained.
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
prefix	string	A prefix that is matched against object-names within a bucket.
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

rules

Information about the lifecycle management rule of a bucket.

Name	Type	Description
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
bucket_name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
name	string	Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
object_filter	object_filter	Specifies a way to filter objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

Name	Type	Description
rules	array[rules]	Specifies an object store lifecycle management policy.

s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

Name	Type	Description
delimiters	array[string]	An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.
max_keys	array[integer]	An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.
operator	string	Condition operator that is applied to the specified condition key.
prefixes	array[string]	An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.

Name	Type	Description
source_ips	array[string]	An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.
usernames	array[string]	An array of usernames that a current user in the context is evaluated against using the condition operators.

s3_bucket_policy_statement

Specifies information about a single access permission.

Name	Type	Description
actions	array[string]	
conditions	array[s3_bucket_policy_condition]	Specifies bucket policy conditions.
effect	string	Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
principals	array[string]	
resources	array[string]	
sid	string	Specifies the statement identifier used to differentiate between statements. The sid length can range from 1 to 256 characters and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The

user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

Name	Type	Description
statements	array[s3_bucket_policy_statemen t]	Specifies bucket access policy statement.

destination

Name	Type	Description
is_cloud	boolean	Specifies whether a bucket is protected within the Cloud. This field cannot be specified using a POST method.
is_external_cloud	boolean	Specifies whether a bucket is protected on external Cloud providers. This field cannot be specified using a POST method.
is_ontap	boolean	Specifies whether a bucket is protected within ONTAP. This field cannot be specified using a POST method. <ul style="list-style-type: none">• Default value: 1• readOnly: 1• Introduced in: 9.10• x-nullable: true

protection_status

Specifies attributes of bucket protection.

Name	Type	Description
destination	destination	

Name	Type	Description
is_protected	boolean	<p>Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be specified using a POST method.</p> <ul style="list-style-type: none"> • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

Name	Type	Description
max_throughput	string	<p>Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.</p>
max_throughput_iops	integer	<p>Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.</p>

Name	Type	Description
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.

Name	Type	Description
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

retention

Specifies the retention mode and default retention period configured on the bucket.

Name	Type	Description
default_period	string	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.</num></num>

Name	Type	Description
mode	string	The lock mode of the bucket. compliance ‐ A SnapLock Compliance (SLC) bucket provides the highest level of WORM protection and an administrator cannot destroy a compliance bucket if it contains unexpired WORM objects. governance ‐ An administrator can delete a Governance bucket. no_lock ‐ Indicates the bucket does not support object locking.

snapshot_policy

Specifies the bucket snapshot policy.

Name	Type	Description
name	string	Specifies the name of the snapshot policy.
uuid	string	Specifies the unique identifier of the snapshot policy.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted.

Name	Type	Description
name	string	The name of the volume. This field cannot be specified in a PATCH method.
uuid	string	<p>Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move.</p> <ul style="list-style-type: none"> • example: 028baa66-41bd-11e9-81d5-00a0986138f7 • Introduced in: 9.6 • x-nullable: true

s3_bucket

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

Name	Type	Description
aggregates	array[aggregates]	A list of aggregates for FlexGroup volume constituents where the bucket is hosted. If this option is not specified, the bucket is auto-provisioned as a FlexGroup volume.
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.
audit_event_selector	audit_event_selector	Audit event selector allows you to specify access and permission types to audit.
comment	string	Can contain any additional information about the bucket being created or modified.

Name	Type	Description
constituents_per_aggregate	integer	Specifies the number of constituents or FlexVol volumes per aggregate. A FlexGroup volume consisting of all such constituents across all specified aggregates is created. This option is used along with the aggregates option and cannot be used independently.
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
is_nas_path_mutable	boolean	Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.

Name	Type	Description
lifecycle_management	lifecycle_management	Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.
name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.

Name	Type	Description
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be specified using a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
storage_service_level	string	Specifies the storage service level of the FlexGroup volume on which the bucket should be created. Valid values are "value", "performance" or "extreme".
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Specifies the bucket type. Valid values are "s3" and "nas".

Name	Type	Description
use_mirrored_aggregates	boolean	Specifies whether mirrored aggregates are selected when provisioning a FlexGroup. Only mirrored aggregates are used if this parameter is set to "true" and only unmirrored aggregates are used if this parameter is set to "false". The default value is "true" for a MetroCluster configuration and is "false" for a non-MetroCluster configuration.
uuid	string	Specifies the unique identifier of the bucket.
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted.

job_link

Name	Type	Description
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete the S3 bucket configuration for an SVM

```
DELETE /protocols/s3/buckets/{svm.uuid}/{uuid}
```

Introduced In: 9.8

Deletes the S3 bucket configuration of an SVM. An access policy is also deleted on an S3 bucket "delete" command.

Related ONTAP commands

- `vserver object-store-server bucket delete`
- `vserver object-store-server bucket policy statement delete`
- `vserver object-store-server bucket policy-statement-condition delete`
- `vserver object-store-server bucket lifecycle-management-rule delete`
- `vserver object-store-server bucket cors-rule delete`

Learn more

- [DOC /protocols/s3/buckets](#)

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	The unique identifier of the bucket.

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none"> • Default value: 0 • Max value: 120 • Min value: 0
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Response

Status: 200, Ok

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "string"
  }
}
```

Response

Status: 202, Accepted

Error

Status: Default

ONTAP Error Response Codes

Error code	Message
92405811	"Failed to delete bucket "{bucket name}" for SVM "{svm.name}". Wait a few minutes and try the operation again.";
92405858	"Failed to "delete" the "bucket" because the operation is only supported on data SVMs.";
92405861	"The specified SVM UUID or bucket UUID does not exist.";
92405779	"Failed to remove bucket "{bucket name}" for SVM "{svm.name}". Reason: {Reason for failure}. ";
92405813	"Failed to delete the object store volume. Reason: {Reason for failure}.";
92405864	"An error occurred when deleting an access policy. The reason for failure is detailed in the error message.";

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

job_link

Name	Type	Description
_links	_links	
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve the S3 bucket configuration for an SVM

GET /protocols/s3/buckets/{svm.uuid}/{uuid}

Introduced In: 9.8

Retrieves the S3 bucket configuration of an SVM. Note that in order to retrieve S3 bucket policy conditions, the 'fields' option should be set to `***`.

Related ONTAP commands

- `vserver object-store-server bucket show`
- `vserver object-store-server bucket policy statement show`
- `vserver object-store-server bucket policy-statement-condition show`
- `vserver object-store-server bucket lifecycle-management-rule show`
- `vserver object-store-server bucket cors-rule show`

Learn more

- [DOC /protocols/s3/buckets](#)

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	The unique identifier of the bucket.
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.

Response

Status: 200, Ok

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.
audit_event_selector	audit_event_selector	Audit event selector allows you to specify access and permission types to audit.

Name	Type	Description
comment	string	Can contain any additional information about the bucket being created or modified.
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
is_nas_path_mutable	boolean	Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.
lifecycle_management	lifecycle_management	Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

Name	Type	Description
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.
name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.

Name	Type	Description
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be specified using a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Specifies the bucket type. Valid values are "s3" and "nas".
uuid	string	Specifies the unique identifier of the bucket.

Name	Type	Description
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted.

Example response

```
{
  "audit_event_selector": {
    "access": "string",
    "permission": "string"
  },
  "comment": "S3 bucket.",
  "cors": {
    "rules": [
      {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "allowed_headers": [
          "x-amz-request-id"
        ],
        "allowed_methods": [
          "PUT",
          "DELETE"
        ],
        "allowed_origins": [
          "http://www.example.com"
        ],
        "expose_headers": [
          "x-amz-date"
        ],
        "id": "string",
        "max_age_seconds": 1024
      }
    ]
  },
  "lifecycle_management": {
    "rules": [
      {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "abort_incomplete_multipart_upload": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          }
        }
      }
    ]
  }
}
```



```

    }
  },
  "bucket_name": "bucket1",
  "expiration": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "object_age_days": 100,
    "object_expiry_date": "2039-09-22 20:00:00 -0400"
  },
  "name": "string",
  "non_current_version_expiration": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "object_filter": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "prefix": "/logs",
    "size_greater_than": 10240,
    "size_less_than": 10485760,
    "tags": [
      "project1=projA",
      "project2=projB"
    ]
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055"
}

```

```

    ]
  },
  "logical_used_size": 0,
  "name": "bucket1",
  "nas_path": "/",
  "policy": {
    "statements": [
      {
        "actions": [
          "GetObject",
          "PutObject",
          "DeleteObject",
          "ListBucket"
        ],
        "conditions": [
          {
            "delimiters": [
              "/"
            ],
            "max_keys": [
              1000
            ],
            "operator": "ip_address",
            "prefixes": [
              "pref"
            ],
            "source_ips": [
              "1.1.1.1",
              "1.2.2.0/24"
            ],
            "usernames": [
              "user1"
            ]
          }
        ],
        "effect": "allow",
        "principals": [
          "user1",
          "group/grp1",
          "nasgroup/group1"
        ],
        "resources": [
          "bucket1",
          "bucket1/*"
        ],
        "sid": "FullAccessToUser1"
      }
    ]
  }
}

```

```

    }
  ],
},
"qos_policy": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
},
"max_throughput": [
  "900KB/s",
  "500MB/s",
  "120GB/s",
  "5000IOPS",
  "5000IOPS,500KB/s",
  "2500IOPS,100MB/s",
  "1000IOPS,25MB/s"
],
"max_throughput_iops": 10000,
"max_throughput_mbps": 500,
"min_throughput": [
  "900KB/s",
  "500MB/s",
  "120GB/s",
  "5000IOPS",
  "5000IOPS,500KB/s",
  "2500IOPS,100MB/s",
  "1000IOPS,25MB/s"
],
"min_throughput_iops": 2000,
"min_throughput_mbps": 500,
"name": "performance",
"uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"retention": {
  "default_period": "P10Y",
  "mode": "governance"
},
"role": "string",
"size": 1677721600,
"snapshot_policy": {
  "name": "default-1weekly",
  "uuid": "3675af31-431c-12fa-114a-20675afebc12"
},
"svm": {
  "_links": {

```

```

    "self": {
      "href": "/api/resourcelink"
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "type": "s3",
  "use_mirrored_aggregates": true,
  "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055",
  "versioning_state": "enabled",
  "volume": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "volume1",
    "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
  }
}

```

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

aggregates

Aggregate

Name	Type	Description
_links	_links	
name	string	
uuid	string	

audit_event_selector

Audit event selector allows you to specify access and permission types to audit.

Name	Type	Description
access	string	Specifies read and write access types.
permission	string	Specifies allow and deny permission types.

rules

Information about the CORS rule of an S3 bucket.

Name	Type	Description
_links	_links	
allowed_headers	array[string]	An array of HTTP headers allowed in the cross-origin requests.
allowed_methods	array[string]	An array of HTTP methods allowed in the cross-origin requests.

Name	Type	Description
allowed_origins	array[string]	List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.
expose_headers	array[string]	List of extra headers sent in the response that customers can access from their applications.
id	string	Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
max_age_seconds	integer	The time in seconds for your browser to cache the preflight response for the specified resource.

cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
rules	array[rules]	Specifies an object store bucket CORS rule.

encryption

Name	Type	Description
enabled	boolean	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be specified in a POST method.

abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
_links	_links	

Name	Type	Description
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
new_non_current_versions	integer	Number of latest non-current versions to be retained.
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
_links	_links	
prefix	string	A prefix that is matched against object-names within a bucket.

Name	Type	Description
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

rules

Information about the lifecycle management rule of a bucket.

Name	Type	Description
_links	_links	
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
bucket_name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
name	string	Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
object_filter	object_filter	Specifies a way to filter objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

Name	Type	Description
rules	array[rules]	Specifies an object store lifecycle management policy.

s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

Name	Type	Description
delimiters	array[string]	An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.
max_keys	array[integer]	An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.
operator	string	Condition operator that is applied to the specified condition key.
prefixes	array[string]	An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.
source_ips	array[string]	An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.
usernames	array[string]	An array of usernames that a current user in the context is evaluated against using the condition operators.

s3_bucket_policy_statement

Specifies information about a single access permission.

Name	Type	Description
actions	array[string]	
conditions	array[s3_bucket_policy_condition]	Specifies bucket policy conditions.

Name	Type	Description
effect	string	Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
principals	array[string]	
resources	array[string]	
sid	string	Specifies the statement identifier used to differentiate between statements. The sid length can range from 1 to 256 characters and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

Name	Type	Description
statements	array[s3_bucket_policy_statement]	Specifies bucket access policy statement.

destination

Name	Type	Description
is_cloud	boolean	Specifies whether a bucket is protected within the Cloud. This field cannot be specified using a POST method.
is_external_cloud	boolean	Specifies whether a bucket is protected on external Cloud providers. This field cannot be specified using a POST method.

Name	Type	Description
is_ontap	boolean	<p>Specifies whether a bucket is protected within ONTAP. This field cannot be specified using a POST method.</p> <ul style="list-style-type: none"> • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

protection_status

Specifies attributes of bucket protection.

Name	Type	Description
destination	destination	
is_protected	boolean	<p>Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be specified using a POST method.</p> <ul style="list-style-type: none"> • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

Name	Type	Description
_links	_links	

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

retention

Specifies the retention mode and default retention period configured on the bucket.

Name	Type	Description
default_period	string	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.</num></num>
mode	string	The lock mode of the bucket. compliance ‐ A SnapLock Compliance (SLC) bucket provides the highest level of WORM protection and an administrator cannot destroy a compliance bucket if it contains unexpired WORM objects. governance ‐ An administrator can delete a Governance bucket. no_lock ‐ Indicates the bucket does not support object locking.

snapshot_policy

Specifies the bucket snapshot policy.

Name	Type	Description
name	string	Specifies the name of the snapshot policy.
uuid	string	Specifies the unique identifier of the snapshot policy.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted.

Name	Type	Description
_links	_links	
name	string	The name of the volume. This field cannot be specified in a PATCH method.
uuid	string	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move. <ul style="list-style-type: none">• example: 028baa66-41bd-11e9-81d5-00a0986138f7• Introduced in: 9.6• x-nullable: true

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array [error_arguments]	Message arguments

Name	Type	Description
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update the S3 bucket configuration for an SVM

PATCH /protocols/s3/buckets/{svm.uuid}/{uuid}

Introduced In: 9.8

Updates the S3 bucket configuration of an SVM.

Important notes

- The following fields can be modified for a bucket:
 - `comment` - Any information related to the bucket.
 - `size` - Bucket size.
 - `policy` - An access policy for resources (buckets and objects) that defines their permissions. New policies are created after existing policies are deleted. To retain any of the existing policy statements, you need to specify those statements again. Also, policy conditions can be specified as part of a bucket policy.
 - `qos_policy` - A QoS policy for buckets.
 - `audit_event_selector` - Audit policy for buckets. None can be specified for both access and permission to remove an audit event selector.
 - `versioning-state` - Versioning state of the buckets.
 - `nas_path` - NAS path to which the bucket corresponds to.
 - `retention.default_period` - Specifies the duration of default-retention applicable for objects on the object store bucket.
 - `cors` - Specifying CORS rules enables the bucket to service the cross-origin requests. Note that the new CORS configuration specified will replace the existing one. If you need to retain any of the existing CORS rules, specify those rules again as part of the new CORS rules. To remove all the existing rules, specify an empty CORS configuration as input.
 - `snapshot_policy` - Snapshot policy for the bucket.

Related ONTAP commands

- `vserver object-store-server bucket modify`
- `vserver object-store-server bucket policy statement modify`
- `vserver object-store-server bucket policy-statement-condition modify`

- `vserver object-store-server bucket cors-rule create`
- `vserver object-store-server bucket cors-rule delete`

Learn more

- [DOC /protocols/s3/buckets](#)

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	The unique identifier of the bucket.
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none"> • Default value: 0 • Max value: 120 • Min value: 0
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.
audit_event_selector	audit_event_selector	Audit event selector allows you to specify access and permission types to audit.
comment	string	Can contain any additional information about the bucket being created or modified.
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.

Name	Type	Description
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps" . Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be specified using a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.

Name	Type	Description
type	string	Specifies the bucket type. Valid values are "s3" and "nas".
uuid	string	Specifies the unique identifier of the bucket.
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted.

Example request

```
{
  "audit_event_selector": {
    "access": "string",
    "permission": "string"
  },
  "comment": "S3 bucket.",
  "cors": {
    "rules": [
      {
        "allowed_headers": [
          "x-amz-request-id"
        ],
        "allowed_methods": [
          "PUT",
          "DELETE"
        ],
        "allowed_origins": [
          "http://www.example.com"
        ],
        "expose_headers": [
          "x-amz-date"
        ],
        "id": "string",
        "max_age_seconds": 1024
      }
    ]
  },
  "is_nas_path_mutable": true,
  "logical_used_size": 0,
  "nas_path": "/",
  "policy": {
    "statements": [
      {
        "actions": [
          "GetObject",
          "PutObject",
          "DeleteObject",
          "ListBucket"
        ],
        "conditions": [
          {
            "delimiters": [
              "/"
            ]
          }
        ]
      }
    ]
  }
}
```

```

        "max_keys": [
            1000
        ],
        "operator": "ip_address",
        "prefixes": [
            "pref"
        ],
        "source_ips": [
            "1.1.1.1",
            "1.2.2.0/24"
        ],
        "usernames": [
            "user1"
        ]
    }
],
"effect": "allow",
"principals": [
    "user1",
    "group/grp1",
    "nasgroup/group1"
],
"resources": [
    "bucket1",
    "bucket1/*"
],
"sid": "FullAccessToUser1"
}
]
},
"qos_policy": {
    "max_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
    ],
    "max_throughput_iops": 10000,
    "max_throughput_mbps": 500,
    "min_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",

```



```

        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
    ],
    "min_throughput_iops": 2000,
    "min_throughput_mbps": 500,
    "name": "performance",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"retention": {
    "default_period": "P10Y"
},
"role": "string",
"size": 1677721600,
"snapshot_policy": {
    "name": "default-1weekly",
    "uuid": "3675af31-431c-12fa-114a-20675afebc12"
},
"type": "s3",
"use_mirrored_aggregates": true,
"uuid": "414b29a1-3b26-11e9-bd58-0050568ea055",
"versioning_state": "enabled",
"volume": {
    "name": "volume1",
    "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
}
}

```

Response

Status: 200, Ok

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "uuid": "string"
  }
}
```

Response

Status: 202, Accepted

Error

Status: Default

ONTAP Error Response Codes

Error code	Message
92405778	"Failed to modify bucket "{bucket name}" for SVM "{svm.name}". Reason: {Reason for failure}. ";
92405846	"Failed to modify the object store volume. Reason: {Reason for failure}.";
92405811	"Failed to modify bucket "{bucket name}" for SVM "{svm.name}". Wait a few minutes and try the operation again.";
92405858	"Failed to "modify" the "bucket" because the operation is only supported on data SVMs.";
92405861	"The specified SVM UUID or bucket UUID does not exist.";
92405863	"An error occurs when creating an access policy. The reason for failure is detailed in the error message.";
92405864	"An error occurs when deleting an access policy. The reason for failure is detailed in the error message.";
92405891	The resources specified in the access policy are not valid. Valid ways to specify a resource are *, <bucket-name>, <bucket-name>/.../.... Valid characters for a resource are 0-9, A-Z, a-z, _, +, comma, ;, :, =, ., &, @, ?, (,), single quote, *, !, - and \$.
92405894	"Statements, principals and resources list can have a maximum of 10 entries.";

Error code	Message
92405897	The principals specified in the access policy are not in the correct format. User name must be in between 1 and 64 characters. Valid characters for a user name are 0-9, A-Z, a-z, _, +, =, comma, ., @, and - .
92405898	"The SID specified in the access policy is not valid. Valid characters for a SID are 0-9, A-Z and a-z.";
92406014	"Failed to modify event selector for bucket "{bucket name}". If the value of either access or permission is set to none, they both must be set to none.";
92733458	"[Job job number] Job failed: Failed to modify bucket "s3bucket1" for SVM "vs1". Reason: {Reason for failure}. ";
8454236	"Could not assign qtree "qtree1" to QoS policy group "group1". Invalid QoS policy group specified "group1". The specified QoS policy group has a min-throughput value set, and the workload being assigned resides on a platform that does not support min-throughput or the cluster is in a mixed version state and the effective cluster version of ONTAP does not support min-throughput on this platform.";
8454323	"Policy group with UUID "23bwegew-8eqg-121r-bjad-0050e628wq732" does not exist."
92406230	"The value for "retention.default_period" parameter for object store bucket "<bucket>" cannot be greater than the maximum lock retention period set in the object store server for SVM "<SVM>". Check the maximum allowed lock retention period present in the object store server for SVM "<SVM>" and try the operation again."; //end row //start row
92406236 //end row //start row	"The value for "retention.default_period" parameter for object store bucket "<bucket>" cannot be less than the minimum lock retention period set in the object store server for SVM "<SVM>". Check the minimum allowed lock retention period present in the object store server for SVM "<SVM>" and try the operation again."; //end row //start row
92406217 //end row //start row	"The specified "allowed_headers" is not valid because it contains more than one wild card ("*") character."; //end row //start row
92406224 //end row //start row	"A Cross-Origin Resource Sharing (CORS) rule must have an origin and HTTP method specified."; //end row //start row

Error code	Message
92406222 //end row //start row	"Cannot specify Cross-Origin Resource Sharing (CORS) configuration for object store bucket "<bucket>" on SVM "<SVM>". Specifying such configuration is supported on object store volumes created in ONTAP 9.8 or later releases only."; //end row //start row
92406211 //end row //start row	"The specified method "DONE" is not valid. Valid methods are GET, PUT, DELETE, HEAD, and POST."; //end row //start row
92405863 //end row //start row	"Failed to create CORS rules for bucket "bb1". Reason: "Field "index" cannot be specified for this operation.". Resolve all the issues and retry the operation."; //end row //start row
92406228 //end row //start row	"Cannot exceed the maximum limit of 100 Cross-Origin Resource Sharing (CORS) rules per S3 bucket "<bucket>" in SVM "<SVM>"."; //end row

|Name |Type |Description

|href |string a|

[#_links] [.api-collapsible-fifth-title] _links [#aggregates] [.api-collapsible-fifth-title] aggregates
Aggregate
[cols=3*,options=header]

|Name |Type |Description

|name |string a|

|uuid |string a|

[#audit_event_selector] [.api-collapsible-fifth-title] audit_event_selector
Audit event selector allows you to specify access and permission types to audit.
[cols=3*,options=header]

|Name |Type |Description

|access |string a|Specifies read and write access types.

|permission |string a|Specifies allow and deny permission types.

[#rules] [.api-collapsible-fifth-title] rules

Information about the CORS rule of an S3 bucket.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

allowed_headers	array[string]	a An array of HTTP headers allowed in the cross-origin requests.
-----------------	---------------	--

allowed_methods	array[string]	a An array of HTTP methods allowed in the cross-origin requests.
-----------------	---------------	--

allowed_origins	array[string]	a List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.
-----------------	---------------	---

expose_headers	array[string]	a List of extra headers sent in the response that customers can access from their applications.
----------------	---------------	---

id	string	a Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
----	--------	---

max_age_seconds	integer	a The time in seconds for your browser to cache the preflight response for the specified resource.
-----------------	---------	--

[#cors] [.api-collapsible-fifth-title] cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

rules	array[rules]	a Specifies an object store bucket CORS rule.
-------	--------------------------------	---

[#encryption] [.api-collapsible-fifth-title] encryption

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

enabled	boolean	a Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be specified in a POST method.
---------	---------	---

[#abort_incomplete_multipart_upload] [.api-collapsible-fifth-title] abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

[cols=3*,options=header]

|Name |Type |Description

|after_initiation_days |integer a|Number of days of initiation after which uploads can be aborted.

[#expiration] [.api-collapsible-fifth-title] expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

[cols=3*,options=header]

|Name |Type |Description

|expired_object_delete_marker |boolean a|Cleanup object delete markers.

|object_age_days |integer a|Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.

|object_expiry_date |string a|Specific date from when objects can expire. This cannot be used with object_age_days.

[#non_current_version_expiration] [.api-collapsible-fifth-title] non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

[cols=3*,options=header]

|Name |Type |Description

|new_non_current_versions |integer a|Number of latest non-current versions to be retained.

|non_current_days |integer a|Number of days after which non-current versions can be deleted.

[#object_filter] [.api-collapsible-fifth-title] object_filter

Specifies a way to filter objects within a bucket.

[cols=3*,options=header]

|Name |Type |Description

|prefix |string a|A prefix that is matched against object-names within a bucket.

|size_greater_than |integer a|Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.

|size_less_than |integer a|Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.

|tags |array[string] a|An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

[#svm] [.api-collapsible-fifth-title] svm

Specifies the name of the SVM where this bucket exists.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

name	string a	The name of the SVM. This field cannot be specified in a PATCH method.
------	----------	--

uuid	string a	The unique identifier of the SVM. This field cannot be specified in a PATCH method.
------	----------	---

[#rules] [.api-collapsible-fifth-title] rules

Information about the lifecycle management rule of a bucket.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

abort_incomplete_multipart_upload	abort_incomplete_multipart_upload a	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
-----------------------------------	---	--

enabled	boolean a	Specifies whether or not the associated rule is enabled.
---------	-----------	--

expiration	expiration a	Specifies a way to perform expiration action on filtered objects within a bucket.
------------	------------------------------	---

non_current_version_expiration	non_current_version_expiration a	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
--------------------------------	--	---

svm	svm a	Specifies the name of the SVM where this bucket exists.
-----	-----------------------	---

uuid	string a	Specifies the unique identifier of the bucket.
------	----------	--

[#lifecycle_management] [.api-collapsible-fifth-title] lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

rules	array[rules] a	Specifies an object store lifecycle management policy.
-------	----------------------------------	--

[#s3_bucket_policy_condition] [.api-collapsible-fifth-title] s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

|delimiters |array[string] a|An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.

|max_keys |array[integer] a|An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.

|operator |string a|Condition operator that is applied to the specified condition key.

|prefixes |array[string] a|An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.

|source_ips |array[string] a|An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.

|usernames |array[string] a|An array of usernames that a current user in the context is evaluated against using the condition operators.

[#s3_bucket_policy_statement] [.api-collapsible-fifth-title] s3_bucket_policy_statement

Specifies information about a single access permission.

[cols=3*,options=header]

|Name |Type |Description

|actions |array[string] a|

|conditions |array[s3_bucket_policy_condition] a|Specifies bucket policy conditions.

|effect |string a|Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.

|principals |array[string] a|

|resources |array[string] a|

|sid |string a|Specifies the statement identifier used to differentiate between statements. The sid length can range from 1 to 256 characters and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

[#policy] [.api-collapsible-fifth-title] policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

[cols=3*,options=header]

|Name |Type |Description

|statements |array[s3_bucket_policy_statement] a|Specifies bucket access policy statement.

[#destination] [.api-collapsible-fifth-title] destination

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

is_cloud	boolean a	Specifies whether a bucket is protected within the Cloud. This field cannot be specified using a POST method.
----------	-----------	---

is_external_cloud	boolean a	Specifies whether a bucket is protected on external Cloud providers. This field cannot be specified using a POST method.
-------------------	-----------	--

is_ontap	boolean a	Specifies whether a bucket is protected within ONTAP. This field cannot be specified using a POST method.
----------	-----------	---

- Default value: 1
- readOnly: 1
- Introduced in: 9.10
- x-nullable: true

[#protection_status] [.api-collapsible-fifth-title] protection_status

Specifies attributes of bucket protection.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

destination	destination a	
-------------	-------------------------------	--

is_protected	boolean a	Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be specified using a POST method.
--------------	-----------	--

- Default value: 1
- readOnly: 1
- Introduced in: 9.10
- x-nullable: true

[#qos_policy] [.api-collapsible-fifth-title] qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

|max_throughput |string a|Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

|max_throughput_iops |integer a|Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.

|max_throughput_mbps |integer a|Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.

|min_throughput |string a|Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

|min_throughput_iops |integer a|Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.

|min_throughput_mbps |integer a|Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.

|name |string a|The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.

|uuid |string a|The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

[#retention] [.api-collapsible-fifth-title] retention

Specifies the retention mode and default retention period configured on the bucket.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

default_period string a	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.
--------------------------	--

[#snapshot_policy] [.api-collapsible-fifth-title] snapshot_policy

Specifies the bucket snapshot policy.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

name	string a	Specifies the name of the snapshot policy.
------	----------	--

uuid	string a	Specifies the unique identifier of the snapshot policy.
------	----------	---

[#svm] [.api-collapsible-fifth-title] svm

SVM, applies only to SVM-scoped objects.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

name	string a	The name of the SVM. This field cannot be specified in a PATCH method.
------	----------	--

uuid	string a	The unique identifier of the SVM. This field cannot be specified in a PATCH method.
------	----------	---

[#volume] [.api-collapsible-fifth-title] volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

name	string a	The name of the volume. This field cannot be specified in a PATCH method.
------	----------	---

uuid	string a	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move.
------	----------	---

- example: 028baa66-41bd-11e9-81d5-00a0986138f7
- Introduced in: 9.6
- x-nullable: true

[#s3_bucket] [.api-collapsible-fifth-title] s3_bucket

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

allowed	boolean a	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.
---------	-----------	---

|audit_event_selector |[audit_event_selector](#) a|Audit event selector allows you to specify access and permission types to audit.

|comment |string a|Can contain any additional information about the bucket being created or modified.

|cors |[cors](#) a|Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

|encryption |[encryption](#) a|

|is_consistent_etag |boolean a|Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.

|logical_used_size |integer a|Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.

|nas_path |string a|Specifies the NAS path to which the nas bucket corresponds to.

|policy |[policy](#) a|A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

|protection_status |[protection_status](#) a|Specifies attributes of bucket protection.

|qos_policy |[qos_policy](#) a|Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

|retention |[retention](#) a|Specifies the retention mode and default retention period configured on the bucket.

|role |string a|Specifies the role of the bucket. This field cannot be specified using a POST method.

|size |integer a|Specifies the bucket size in bytes; ranges from 190MB to 62PB.

|snapshot_policy |[snapshot_policy](#) a|Specifies the bucket snapshot policy.

|type |string a|Specifies the bucket type. Valid values are "s3" and "nas".

|uuid |string a|Specifies the unique identifier of the bucket.

|versioning_state |string a|Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.

|volume |[volume](#) a|Specifies the FlexGroup volume name and UUID where the bucket is hosted.

[#job_link] [.api-collapsible-fifth-title] job_link

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

uuid	string a	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.
------	----------	---

#error_arguments

[.api-collapsible-fifth-title] error_arguments

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

code	string a	Argument code
------	----------	---------------

message	string a	Message argument
---------	----------	------------------

#returned_error

[.api-collapsible-fifth-title] returned_error

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

arguments	array[error_arguments] a	Message arguments
-----------	--	-------------------

code	string a	Error code
------	----------	------------

message	string a	Error message
---------	----------	---------------

target	string a	The target parameter that caused the error.
--------	----------	---

====

:leveloffset: -1

= Manage protocols S3 services

:leveloffset: 1

[[IDc8f6cda5845b60cc38ee535fbb3bdb08]] = Manage protocols S3 services

== Overview

An S3 server is an object store server that is compatible with the Amazon S3 protocol. In the initial version, only a subset of the protocol features necessary to support Fabric Pool capacity tier usecases are implemented. S3 server allows you to store objects in ONTAP using Amazon S3 protocol. This feature can be used as a target object store server for ONTAP FabricPools.

== Performance monitoring

Performance of the SVM can be monitored by the ``metric.`` and ``statistics.`` properties. These show the performance of the SVM in terms of IOPS, latency and throughput. The ``metric.`` **properties denote an average whereas** ``statistics.`` properties denote a real-time monotonically increasing value aggregated across all nodes.

== Examples

=== Retrieving all of the S3 configurations

The API: /api/protocols/s3/services

The call: curl -X GET "https://<mgmt-ip>/api/protocols/s3/services?fields=*&return_records=true&return_timeout=15" -H "accept: application/json"

The response: { "records": [{ "svm": { "uuid": "cf90b8f2-8071-11e9-8190-0050568eae21", "name": "vs2" }, "name": "vs1", "comment": "S3 server", "enabled": false, "max_lock_retention_period": "none", "min_lock_retention_period": "none" }, { "svm": { "uuid": "d7f1219c-7f8e-11e9-9124-0050568eae21", "name": "vs1" }, "name": "Server-1", "comment": "S3 server", "enabled": true, "max_lock_retention_period": "none", "min_lock_retention_period": "none", "buckets": [{ "uuid": "e08665af-8114-11e9-8190-0050568eae21", "name": "bucket-1", "volume": { "name": "fg_oss_1559026220", "uuid": "de146bff-8114-11e9-8190-0050568eae21" }, "size": 209715200, "logical_used_size": 157286400, "encryption": { "enabled": false }, "comment": "s3 bucket" }, { "uuid": "fb1912ef-8114-11e9-8190-0050568eae21", "name": "bucket-2", "volume": { "name": "fg_oss_1559026269", "uuid": "f9b1cdd0-8114-11e9-8190-0050568eae21" }, "size": 1048576000, "logical_used_size": 78643200, "encryption": { "enabled": false }, "comment": "s3 bucket" }], "users": [{ "name": "user-1", "comment": "S3 user", "access_key": "<AWS-ACCESS-KEY-ID>" }, { "name": "user-2", "comment": "", "access_key": "<AWS-ACCESS-KEY-ID>" }] }, "num_records": 2 } ----

=== Retrieving all S3 configurations for a particular SVM

The API: /api/protocols/s3/services/{svm.uuid}

|Name |Type |In |Required |Description

|users.key_expiry_time |string |query |False a|Filter by users.key_expiry_time

- Introduced in: 9.14

|users.name |string |query |False a|Filter by users.name

- maxLength: 64
- minLength: 1

|users.svm.name |string |query |False a|Filter by users.svm.name

|users.svm.uuid |string |query |False a|Filter by users.svm.uuid

|users.comment |string |query |False a|Filter by users.comment

- maxLength: 256
- minLength: 0

|users.key_time_to_live |string |query |False a|Filter by users.key_time_to_live

- Introduced in: 9.14

|users.access_key |string |query |False a|Filter by users.access_key

|certificate.name |string |query |False a|Filter by certificate.name

- Introduced in: 9.8

|certificate.uuid |string |query |False a|Filter by certificate.uuid

- Introduced in: 9.8

|svm.name |string |query |False a|Filter by svm.name

|svm.uuid |string |query |False a|Filter by svm.uuid

|is_https_enabled |boolean |query |False a|Filter by is_https_enabled

- Introduced in: 9.8

|metric.iops.other |integer |query |False a|Filter by metric.iops.other

- Introduced in: 9.8

|metric.iops.total |integer |query |False a|Filter by metric.iops.total

- Introduced in: 9.8

|metric.iops.read |integer |query |False a|Filter by metric.iops.read

- Introduced in: 9.8

|metric.iops.write |integer |query |False a|Filter by metric.iops.write

- Introduced in: 9.8

|metric.status |string |query |False a|Filter by metric.status

- Introduced in: 9.8

|metric.latency.other |integer |query |False a|Filter by metric.latency.other

- Introduced in: 9.8

|metric.latency.total |integer |query |False a|Filter by metric.latency.total

- Introduced in: 9.8

|metric.latency.read |integer |query |False a|Filter by metric.latency.read

- Introduced in: 9.8

|metric.latency.write |integer |query |False a|Filter by metric.latency.write

- Introduced in: 9.8

|metric.duration |string |query |False a|Filter by metric.duration

- Introduced in: 9.8

|metric.timestamp |string |query |False a|Filter by metric.timestamp

- Introduced in: 9.8

|metric.throughput.read |integer |query |False a|Filter by metric.throughput.read

- Introduced in: 9.8

|metric.throughput.total |integer |query |False a|Filter by metric.throughput.total

- Introduced in: 9.8

|metric.throughput.write |integer |query |False a|Filter by metric.throughput.write

- Introduced in: 9.8

|comment |string |query |False a|Filter by comment

- maxLength: 256
- minLength: 0

|secure_port |integer |query |False a|Filter by secure_port

- Introduced in: 9.8
- Max value: 65535
- Min value: 1

|default_unix_user |string |query |False a|Filter by default_unix_user

- Introduced in: 9.12

|port |integer |query |False a|Filter by port

- Introduced in: 9.8
- Max value: 65535
- Min value: 1

|buckets.svm.name |string |query |False a|Filter by buckets.svm.name

|buckets.svm.uuid |string |query |False a|Filter by buckets.svm.uuid

|buckets.lifecycle_management.rules.uuid |string |query |False a|Filter by
buckets.lifecycle_management.rules.uuid

- Introduced in: 9.14

|buckets.lifecycle_management.rules.name |string |query |False a|Filter by
buckets.lifecycle_management.rules.name

- Introduced in: 9.13
- maxLength: 256
- minLength: 0

|buckets.lifecycle_management.rules.bucket_name |string |query |False a|Filter by
buckets.lifecycle_management.rules.bucket_name

- Introduced in: 9.14
- maxLength: 63
- minLength: 3

|buckets.lifecycle_management.rules.non_current_version_expiration.new_non_current_versions |integer
|query |False a|Filter by
buckets.lifecycle_management.rules.non_current_version_expiration.new_non_current_versions

- Introduced in: 9.13

|buckets.lifecycle_management.rules.non_current_version_expiration.non_current_days |integer |query |False
a|Filter by buckets.lifecycle_management.rules.non_current_version_expiration.non_current_days

- Introduced in: 9.13

|buckets.lifecycle_management.rules.expiration.object_age_days |integer |query |False a|Filter by
buckets.lifecycle_management.rules.expiration.object_age_days

- Introduced in: 9.13

|buckets.lifecycle_management.rules.expiration.expired_object_delete_marker |boolean |query |False a|Filter
by buckets.lifecycle_management.rules.expiration.expired_object_delete_marker

- Introduced in: 9.13

|buckets.lifecycle_management.rules.expiration.object_expiry_date |string |query |False a|Filter by

buckets.lifecycle_management.rules.expiration.object_expiry_date

- Introduced in: 9.13

|buckets.lifecycle_management.rules.object_filter.tags |string |query |False a|Filter by
buckets.lifecycle_management.rules.object_filter.tags

- Introduced in: 9.13

|buckets.lifecycle_management.rules.object_filter.prefix |string |query |False a|Filter by
buckets.lifecycle_management.rules.object_filter.prefix

- Introduced in: 9.13

|buckets.lifecycle_management.rules.object_filter.size_greater_than |integer |query |False a|Filter by
buckets.lifecycle_management.rules.object_filter.size_greater_than

- Introduced in: 9.13

|buckets.lifecycle_management.rules.object_filter.size_less_than |integer |query |False a|Filter by
buckets.lifecycle_management.rules.object_filter.size_less_than

- Introduced in: 9.13

|buckets.lifecycle_management.rules.enabled |boolean |query |False a|Filter by
buckets.lifecycle_management.rules.enabled

- Introduced in: 9.13

|buckets.lifecycle_management.rules.abort_incomplete_multipart_upload.after_initiation_days |integer |query
|False a|Filter by buckets.lifecycle_management.rules.abort_incomplete_multipart_upload.after_initiation_days

- Introduced in: 9.13

|buckets.lifecycle_management.rules.svm.name |string |query |False a|Filter by
buckets.lifecycle_management.rules.svm.name

- Introduced in: 9.14

|buckets.lifecycle_management.rules.svm.uuid |string |query |False a|Filter by
buckets.lifecycle_management.rules.svm.uuid

- Introduced in: 9.14

|buckets.comment |string |query |False a|Filter by buckets.comment

- maxLength: 256
- minLength: 0

|buckets.encryption.enabled |boolean |query |False a|Filter by buckets.encryption.enabled

|buckets.policy.statements.resources |string |query |False a|Filter by buckets.policy.statements.resources

- Introduced in: 9.8

|buckets.policy.statements.actions |string |query |False a|Filter by buckets.policy.statements.actions

- Introduced in: 9.8

|buckets.policy.statements.effect |string |query |False a|Filter by buckets.policy.statements.effect

- Introduced in: 9.8

|buckets.policy.statements.conditions.usernames |string |query |False a|Filter by buckets.policy.statements.conditions.usernames

- Introduced in: 9.8

|buckets.policy.statements.conditions.source_ips |string |query |False a|Filter by buckets.policy.statements.conditions.source_ips

- Introduced in: 9.8

|buckets.policy.statements.conditions.max_keys |integer |query |False a|Filter by buckets.policy.statements.conditions.max_keys

- Introduced in: 9.8

|buckets.policy.statements.conditions.delimiters |string |query |False a|Filter by buckets.policy.statements.conditions.delimiters

- Introduced in: 9.8

|buckets.policy.statements.conditions.operator |string |query |False a|Filter by buckets.policy.statements.conditions.operator

- Introduced in: 9.8

|buckets.policy.statements.conditions.prefixes |string |query |False a|Filter by buckets.policy.statements.conditions.prefixes

- Introduced in: 9.8

|buckets.policy.statements.principals |string |query |False a|Filter by buckets.policy.statements.principals

- Introduced in: 9.8

|buckets.policy.statements.sid |string |query |False a|Filter by buckets.policy.statements.sid

- Introduced in: 9.8
- maxLength: 256
- minLength: 0

|buckets.qos_policy.min_throughput_mbps |integer |query |False a|Filter by buckets.qos_policy.min_throughput_mbps

- Introduced in: 9.8
- Max value: 4194303
- Min value: 0

|buckets.qos_policy.max_throughput_mbps |integer |query |False a|Filter by

buckets.qos_policy.max_throughput_mbps

- Introduced in: 9.8
- Max value: 4194303
- Min value: 0

|buckets.qos_policy.name |string |query |False a|Filter by buckets.qos_policy.name

- Introduced in: 9.8

|buckets.qos_policy.uuid |string |query |False a|Filter by buckets.qos_policy.uuid

- Introduced in: 9.8

|buckets.qos_policy.max_throughput |string |query |False a|Filter by buckets.qos_policy.max_throughput

- Introduced in: 9.17

|buckets.qos_policy.max_throughput_iops |integer |query |False a|Filter by
buckets.qos_policy.max_throughput_iops

- Introduced in: 9.8
- Max value: 2147483647
- Min value: 0

|buckets.qos_policy.min_throughput_iops |integer |query |False a|Filter by
buckets.qos_policy.min_throughput_iops

- Introduced in: 9.8
- Max value: 2147483647
- Min value: 0

|buckets.qos_policy.min_throughput |string |query |False a|Filter by buckets.qos_policy.min_throughput

- Introduced in: 9.17

|buckets.role |string |query |False a|Filter by buckets.role

- Introduced in: 9.10

|buckets.size |integer |query |False a|Filter by buckets.size

- Max value: 62672162783232000
- Min value: 199229440

|buckets.is_nas_path_mutable |boolean |query |False a|Filter by buckets.is_nas_path_mutable

- Introduced in: 9.17

|buckets.uuid |string |query |False a|Filter by buckets.uuid

|buckets.logical_used_size |integer |query |False a|Filter by buckets.logical_used_size

|buckets.allowed |boolean |query |False a|Filter by buckets.allowed

- Introduced in: 9.12

|buckets.versioning_state |string |query |False a|Filter by buckets.versioning_state

- Introduced in: 9.11

|buckets.cors.rules.expose_headers |string |query |False a|Filter by buckets.cors.rules.expose_headers

- Introduced in: 9.16

|buckets.cors.rules.max_age_seconds |integer |query |False a|Filter by buckets.cors.rules.max_age_seconds

- Introduced in: 9.16

|buckets.cors.rules.allowed_origins |string |query |False a|Filter by buckets.cors.rules.allowed_origins

- Introduced in: 9.16

|buckets.cors.rules.allowed_methods |string |query |False a|Filter by buckets.cors.rules.allowed_methods

- Introduced in: 9.16

|buckets.cors.rules.allowed_headers |string |query |False a|Filter by buckets.cors.rules.allowed_headers

- Introduced in: 9.16

|buckets.cors.rules.id |string |query |False a|Filter by buckets.cors.rules.id

- Introduced in: 9.16
- maxLength: 256
- minLength: 0

|buckets.nas_path |string |query |False a|Filter by buckets.nas_path

- Introduced in: 9.12

|buckets.retention.mode |string |query |False a|Filter by buckets.retention.mode

- Introduced in: 9.14

|buckets.retention.default_period |string |query |False a|Filter by buckets.retention.default_period

- Introduced in: 9.14

|buckets.snapshot_policy.uuid |string |query |False a|Filter by buckets.snapshot_policy.uuid

- Introduced in: 9.16

|buckets.snapshot_policy.name |string |query |False a|Filter by buckets.snapshot_policy.name

- Introduced in: 9.16

|buckets.audit_event_selector.permission |string |query |False a|Filter by

buckets.audit_event_selector.permission

- Introduced in: 9.10

|buckets.audit_event_selector.access |string |query |False a|Filter by buckets.audit_event_selector.access

- Introduced in: 9.10

|buckets.protection_status.is_protected |boolean |query |False a|Filter by
buckets.protection_status.is_protected

- Introduced in: 9.10

|buckets.protection_status.destination.is_ontap |boolean |query |False a|Filter by
buckets.protection_status.destination.is_ontap

- Introduced in: 9.10

|buckets.protection_status.destination.is_external_cloud |boolean |query |False a|Filter by
buckets.protection_status.destination.is_external_cloud

- Introduced in: 9.12

|buckets.protection_status.destination.is_cloud |boolean |query |False a|Filter by
buckets.protection_status.destination.is_cloud

- Introduced in: 9.10

|buckets.type |string |query |False a|Filter by buckets.type

- Introduced in: 9.12

|buckets.volume.uuid |string |query |False a|Filter by buckets.volume.uuid

|buckets.volume.name |string |query |False a|Filter by buckets.volume.name

|buckets.is_consistent_etag |boolean |query |False a|Filter by buckets.is_consistent_etag

- Introduced in: 9.17

|buckets.name |string |query |False a|Filter by buckets.name

- maxLength: 63
- minLength: 3

|statistics.latency_raw.other |integer |query |False a|Filter by statistics.latency_raw.other

- Introduced in: 9.8

|statistics.latency_raw.total |integer |query |False a|Filter by statistics.latency_raw.total

- Introduced in: 9.8

|statistics.latency_raw.read |integer |query |False a|Filter by statistics.latency_raw.read

- Introduced in: 9.8

|statistics.latency_raw.write |integer |query |False a|Filter by statistics.latency_raw.write

- Introduced in: 9.8

|statistics.throughput_raw.read |integer |query |False a|Filter by statistics.throughput_raw.read

- Introduced in: 9.8

|statistics.throughput_raw.total |integer |query |False a|Filter by statistics.throughput_raw.total

- Introduced in: 9.8

|statistics.throughput_raw.write |integer |query |False a|Filter by statistics.throughput_raw.write

- Introduced in: 9.8

|statistics.iops_raw.other |integer |query |False a|Filter by statistics.iops_raw.other

- Introduced in: 9.8

|statistics.iops_raw.total |integer |query |False a|Filter by statistics.iops_raw.total

- Introduced in: 9.8

|statistics.iops_raw.read |integer |query |False a|Filter by statistics.iops_raw.read

- Introduced in: 9.8

|statistics.iops_raw.write |integer |query |False a|Filter by statistics.iops_raw.write

- Introduced in: 9.8

|statistics.status |string |query |False a|Filter by statistics.status

- Introduced in: 9.8

|statistics.timestamp |string |query |False a|Filter by statistics.timestamp

- Introduced in: 9.8

|is_http_enabled |boolean |query |False a|Filter by is_http_enabled

- Introduced in: 9.8

|enabled |boolean |query |False a|Filter by enabled

|min_lock_retention_period |string |query |False a|Filter by min_lock_retention_period

- Introduced in: 9.16

|default_win_user |string |query |False a|Filter by default_win_user

- Introduced in: 9.12

|max_key_time_to_live |string |query |False a|Filter by max_key_time_to_live

- Introduced in: 9.15

|name |string |query |False a|Filter by name

- maxLength: 253
- minLength: 3

|max_lock_retention_period |string |query |False a|Filter by max_lock_retention_period

- Introduced in: 9.16

|fields |array[string] |query |False a|Specify the fields to return.

|max_records |integer |query |False a|Limit the number of records returned.

|return_records |boolean |query |False a|The default is true for GET calls. When set to false, only the number of records is returned.

- Default value: 1

|return_timeout |integer |query |False a|The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.

- Max value: 120
- Min value: 0
- Default value: 15

|order_by |array[string] |query |False a|Order results by specified fields and optional [asc|desc] direction. Default direction is 'asc' for ascending.

== Response

```
` Status: 200, Ok `
```

```
[cols=3*,options=header]
```

|Name |Type |Description

|_links |[collection_links](#) a|

|num_records |integer a|Number of records

|records |array[[s3_service](#)] a|

== Error

```
[cols=3,options=header]
```

|error |[returned_error](#) a|

```
.Example error [%collapsible%closed] ==== [source,json,subs=+macros] { "error": { "arguments": [ { "code":  
"string", "message": "string" } ], "code": "4", "message": "entry doesn't exist", "target": "uuid" } } =====
```

== Definitions

[.api-def-first-level] .See Definitions [%collapsible%closed] ===== [[#href](#)] [.api-collapsible-fifth-title] href

[cols=3*,options=header]

|Name |Type |Description

|href |[string](#) a|

[[#collection_links](#)] [.api-collapsible-fifth-title] collection_links

[cols=3*,options=header]

|Name |Type |Description

|next |[href](#) a|

|self |[href](#) a|

[[#self_link](#)] [.api-collapsible-fifth-title] self_link

[cols=3*,options=header]

|Name |Type |Description

|self |[href](#) a|

[[#_links](#)] [.api-collapsible-fifth-title] _links

[cols=3*,options=header]

|Name |Type |Description

|self |[href](#) a|

[[#aggregates](#)] [.api-collapsible-fifth-title] aggregates

Aggregate

[cols=3*,options=header]

|Name |Type |Description

|_links |[_links](#) a|

|name |[string](#) a|

|uuid |string a|

[#audit_event_selector] [.api-collapsible-fifth-title] audit_event_selector

Audit event selector allows you to specify access and permission types to audit.

[cols=3*,options=header]

|Name |Type |Description

|access |string a|Specifies read and write access types.

|permission |string a|Specifies allow and deny permission types.

[#rules] [.api-collapsible-fifth-title] rules

Information about the CORS rule of an S3 bucket.

[cols=3*,options=header]

|Name |Type |Description

|_links |[_links](#) a|

|allowed_headers |array[string] a|An array of HTTP headers allowed in the cross-origin requests.

|allowed_methods |array[string] a|An array of HTTP methods allowed in the cross-origin requests.

|allowed_origins |array[string] a|List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.

|expose_headers |array[string] a|List of extra headers sent in the response that customers can access from their applications.

|id |string a|Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.

|max_age_seconds |integer a|The time in seconds for your browser to cache the preflight response for the specified resource.

[#cors] [.api-collapsible-fifth-title] cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

[cols=3*,options=header]

|Name |Type |Description

|rules |array[[rules](#)] a|Specifies an object store bucket CORS rule.

[#encryption] [.api-collapsible-fifth-title] encryption

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

enabled	boolean a	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be specified in a POST method.
---------	-----------	---

[#abort_incomplete_multipart_upload] [.api-collapsible-fifth-title] abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links a	
--------	--------------------------	--

after_initiation_days	integer a	Number of days of initiation after which uploads can be aborted.
-----------------------	-----------	--

[#expiration] [.api-collapsible-fifth-title] expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links a	
--------	--------------------------	--

expired_object_delete_marker	boolean a	Cleanup object delete markers.
------------------------------	-----------	--------------------------------

object_age_days	integer a	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
-----------------	-----------	--

object_expiry_date	string a	Specific date from when objects can expire. This cannot be used with object_age_days.
--------------------	----------	---

[#non_current_version_expiration] [.api-collapsible-fifth-title] non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links a	
--------	--------------------------	--

new_non_current_versions	integer a	Number of latest non-current versions to be retained.
--------------------------	-----------	---

non_current_days	integer a	Number of days after which non-current versions can be deleted.
------------------	-----------	---

[#object_filter] [.api-collapsible-fifth-title] object_filter

Specifies a way to filter objects within a bucket.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links	a
--------	------------------------	---

prefix	string a	A prefix that is matched against object-names within a bucket.
--------	----------	--

size_greater_than	integer a	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
-------------------	-----------	--

size_less_than	integer a	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
----------------	-----------	--

tags	array[string] a	An array of key-value paired tags of the form <tag>or <tag=value>.</tag>
------	-----------------	--

[#svm] [.api-collapsible-fifth-title] svm

Specifies the name of the SVM where this bucket exists.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links	a
--------	------------------------	---

name	string a	The name of the SVM. This field cannot be specified in a PATCH method.
------	----------	--

uuid	string a	The unique identifier of the SVM. This field cannot be specified in a PATCH method.
------	----------	---

[#rules] [.api-collapsible-fifth-title] rules

Information about the lifecycle management rule of a bucket.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links	a
--------	------------------------	---

abort_incomplete_multipart_upload	abort_incomplete_multipart_upload a	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
-----------------------------------	---	--

bucket_name	string a	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
-------------	----------	--

enabled	boolean a	Specifies whether or not the associated rule is enabled.
---------	-----------	--

expiration	expiration a	Specifies a way to perform expiration action on filtered objects within a bucket.
------------	------------------------------	---

|name |string a|Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.

|non_current_version_expiration |non_current_version_expiration a|Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

|object_filter |object_filter a|Specifies a way to filter objects within a bucket.

|svm |svm a|Specifies the name of the SVM where this bucket exists.

|uuid |string a|Specifies the unique identifier of the bucket.

[#lifecycle_management] [.api-collapsible-fifth-title] lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

[cols=3*,options=header]

|Name |Type |Description

|rules |array[rules] a|Specifies an object store lifecycle management policy.

[#s3_bucket_policy_condition] [.api-collapsible-fifth-title] s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

[cols=3*,options=header]

|Name |Type |Description

|delimiters |array[string] a|An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.

|max_keys |array[integer] a|An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.

|operator |string a|Condition operator that is applied to the specified condition key.

|prefixes |array[string] a|An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.

|source_ips |array[string] a|An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.

|usernames |array[string] a|An array of usernames that a current user in the context is evaluated against using the condition operators.

[#s3_bucket_policy_statement] [.api-collapsible-fifth-title] s3_bucket_policy_statement

Specifies information about a single access permission.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

actions	array[string]	a
---------	---------------	---

conditions	array[s3_bucket_policy_condition]	a Specifies bucket policy conditions.
------------	-----------------------------------	---------------------------------------

effect	string	a Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
--------	--------	--

principals	array[string]	a
------------	---------------	---

resources	array[string]	a
-----------	---------------	---

sid	string	a Specifies the statement identifier used to differentiate between statements. The sid length can range from 1 to 256 characters and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.
-----	--------	--

[#policy] [.api-collapsible-fifth-title] policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

statements	array[s3_bucket_policy_statement]	a Specifies bucket access policy statement.
------------	-----------------------------------	---

[#destination] [.api-collapsible-fifth-title] destination

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

is_cloud	boolean	a Specifies whether a bucket is protected within the Cloud. This field cannot be specified using a POST method.
----------	---------	---

is_external_cloud	boolean	a Specifies whether a bucket is protected on external Cloud providers. This field cannot be specified using a POST method.
-------------------	---------	--

is_ontap	boolean	a Specifies whether a bucket is protected within ONTAP. This field cannot be specified using a POST method.
----------	---------	---

- Default value: 1
- readOnly: 1
- Introduced in: 9.10
- x-nullable: true

[#protection_status] [.api-collapsible-fifth-title] protection_status

Specifies attributes of bucket protection.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

destination	destination	a
-------------	-----------------------------	---

|is_protected |boolean a|Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be specified using a POST method.

- Default value: 1
- readOnly: 1
- Introduced in: 9.10
- x-nullable: true

[#qos_policy] [.api-collapsible-fifth-title] qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links	a
--------	------------------------	---

|max_throughput |string a|Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

|max_throughput_iops |integer a|Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.

|max_throughput_mbps |integer a|Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.

|min_throughput |string a|Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than

1.

`|min_throughput_iops |integer a|`Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.

`|min_throughput_mbps |integer a|`Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.

`|name |string a|`The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.

`|uuid |string a|`The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

`[#retention] [.api-collapsible-fifth-title] retention`

Specifies the retention mode and default retention period configured on the bucket.

`[cols=3*,options=header]`

`|Name |Type |Description`

`|default_period |string a|`Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.

`|mode |string a|`The lock mode of the bucket. compliance ‐ A SnapLock Compliance (SLC) bucket provides the highest level of WORM protection and an administrator cannot destroy a compliance bucket if it contains unexpired WORM objects. governance ‐ An administrator can delete a Governance bucket. no_lock ‐ Indicates the bucket does not support object locking.

`[#snapshot_policy] [.api-collapsible-fifth-title] snapshot_policy`

Specifies the bucket snapshot policy.

`[cols=3*,options=header]`

`|Name |Type |Description`

`|name |string a|`Specifies the name of the snapshot policy.

`|uuid |string a|`Specifies the unique identifier of the snapshot policy.

[#svm] [.api-collapsible-fifth-title] svm

SVM, applies only to SVM-scoped objects.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

__links	_links	a
---------	------------------------	---

name	string a	The name of the SVM. This field cannot be specified in a PATCH method.
------	----------	--

uuid	string a	The unique identifier of the SVM. This field cannot be specified in a PATCH method.
------	----------	---

[#volume] [.api-collapsible-fifth-title] volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

__links	_links	a
---------	------------------------	---

name	string a	The name of the volume. This field cannot be specified in a PATCH method.
------	----------	---

uuid	string a	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move.
------	----------	---

- example: 028baa66-41bd-11e9-81d5-00a0986138f7
- Introduced in: 9.6
- x-nullable: true

[#s3_bucket] [.api-collapsible-fifth-title] s3_bucket

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

allowed	boolean a	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.
---------	-----------	---

audit_event_selector	audit_event_selector	a	Audit event selector allows you to specify access and permission types to audit.
----------------------	--------------------------------------	---	--

comment	string a	Can contain any additional information about the bucket being created or modified.
---------	----------	--

cors	cors	a	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an
------	----------------------	---	---

origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

|encryption |[encryption](#) a|

|is_consistent_etag |boolean a|Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.

|is_nas_path_mutable |boolean a|Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.

|lifecycle_management |[lifecycle_management](#) a|Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

|logical_used_size |integer a|Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.

|name |string a|Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".

|nas_path |string a|Specifies the NAS path to which the nas bucket corresponds to.

|policy |[policy](#) a|A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

|protection_status |[protection_status](#) a|Specifies attributes of bucket protection.

|qos_policy |[qos_policy](#) a|Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

|retention |[retention](#) a|Specifies the retention mode and default retention period configured on the bucket.

|role |string a|Specifies the role of the bucket. This field cannot be specified using a POST method.

|size |integer a|Specifies the bucket size in bytes; ranges from 190MB to 62PB.

|snapshot_policy |[snapshot_policy](#) a|Specifies the bucket snapshot policy.

|svm |[svm](#) a|SVM, applies only to SVM-scoped objects.

|type |string a|Specifies the bucket type. Valid values are "s3" and "nas".

|uuid |string a|Specifies the unique identifier of the bucket.

|versioning_state |string a|Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.

|volume |[volume](#) a|Specifies the FlexGroup volume name and UUID where the bucket is hosted.

[#certificate] [.api-collapsible-fifth-title] certificate

Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

[cols=3*,options=header]

|Name |Type |Description

|_links |[_links](#) a|

|name |string a|Certificate name

|uuid |string a|Certificate UUID

[#iops] [.api-collapsible-fifth-title] iops

The rate of I/O operations observed at the storage object.

[cols=3*,options=header]

|Name |Type |Description

|other |integer a|Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.

|read |integer a|Performance metric for read I/O operations.

|total |integer a|Performance metric aggregated over all types of I/O operations.

|write |integer a|Performance metric for write I/O operations.

[#latency] [.api-collapsible-fifth-title] latency

The round trip latency in microseconds observed at the storage object.

[cols=3*,options=header]

|Name |Type |Description

|other |integer a|Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.

|read |integer a|Performance metric for read I/O operations.

|total |integer a|Performance metric aggregated over all types of I/O operations.

|write |integer a|Performance metric for write I/O operations.

[#throughput] [.api-collapsible-fifth-title] throughput

The rate of throughput bytes per second observed at the storage object.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

read	integer a	Performance metric for read I/O operations.
------	-----------	---

total	integer a	Performance metric aggregated over all types of I/O operations.
-------	-----------	---

write	integer a	Performance metric for write I/O operations.
-------	-----------	--

[#metric] [.api-collapsible-fifth-title] metric

Performance numbers, such as IOPS latency and throughput, for SVM protocols.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links a
--------	--------------------------

duration	string a	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
----------	----------	--

iops	iops a	The rate of I/O operations observed at the storage object.
------	------------------------	--

latency	latency a	The round trip latency in microseconds observed at the storage object.
---------	---------------------------	--

status	string a	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
--------	----------	---

throughput	throughput a	The rate of throughput bytes per second observed at the storage object.
------------	------------------------------	---

timestamp	string a	The timestamp of the performance data.
-----------	----------	--

[#iops_raw] [.api-collapsible-fifth-title] iops_raw

The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

other	integer a	Performance metric for other I/O operations. Other I/O operations can be metadata operations,
-------	-----------	---

such as directory lookups and so on.

|read |integer a|Performance metric for read I/O operations.

|total |integer a|Performance metric aggregated over all types of I/O operations.

|write |integer a|Performance metric for write I/O operations.

[#latency_raw] [.api-collapsible-fifth-title] latency_raw

The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

[cols=3*,options=header]

|Name |Type |Description

|other |integer a|Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.

|read |integer a|Performance metric for read I/O operations.

|total |integer a|Performance metric aggregated over all types of I/O operations.

|write |integer a|Performance metric for write I/O operations.

[#throughput_raw] [.api-collapsible-fifth-title] throughput_raw

Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

[cols=3*,options=header]

|Name |Type |Description

|read |integer a|Performance metric for read I/O operations.

|total |integer a|Performance metric aggregated over all types of I/O operations.

|write |integer a|Performance metric for write I/O operations.

[#statistics] [.api-collapsible-fifth-title] statistics

These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.

[cols=3*,options=header]

|Name |Type |Description

|iops_raw |[iops_raw](#) a|The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.

|latency_raw |[latency_raw](#) a|The raw latency in microseconds observed at the storage object. This should be

divided by the raw IOPS value to calculate the average latency per I/O operation.

|status |string a|Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.

|throughput_raw |[throughput_raw](#) a|Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

|timestamp |string a|The timestamp of the performance data.

```
[#s3_user] [.api-collapsible-fifth-title] s3_user
```

This is a container of S3 users.

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

access_key	string a	Specifies the access key for the user.
------------	----------	--

comment	string a	Can contain any additional information about the user being created or modified.
---------	----------	--

key_expiry_time	string a	Specifies the date and time after which keys expire and are no longer valid.
-----------------	----------	--

key_time_to_live	string a	Indicates the time period from when this parameter is specified:
------------------	----------	--

- when creating or modifying a user or
- when the user keys were last regenerated, after which the user keys expire and are no longer valid.
- Valid format is: 'PnDTnHnMnS\|PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds.
- If the value specified is '0' seconds, then the keys won't expire.

name	string a	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".
------	----------	---

svm	svm a	SVM, applies only to SVM-scoped objects.
-----	-----------------------	--

```
[#s3_service] [.api-collapsible-fifth-title] s3_service
```

Specifies the S3 server configuration.

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

_links	self_link a	
--------	-----------------------------	--

buckets	array[s3_bucket]	This field cannot be specified in a PATCH method.
---------	------------------------------------	---

|certificate |[certificate](#) a|Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

|comment |string a|Can contain any additional information about the server being created or modified.

|default_unix_user |string a|Specifies the default UNIX user for NAS Access.

|default_win_user |string a|Specifies the default Windows user for NAS Access.

|enabled |boolean a|Specifies whether the S3 server being created or modified should be up or down.

|is_http_enabled |boolean a|Specifies whether HTTP is enabled on the S3 server being created or modified. By default, HTTP is disabled on the S3 server.

|is_https_enabled |boolean a|Specifies whether HTTPS is enabled on the S3 server being created or modified. By default, HTTPS is enabled on the S3 server.

|max_key_time_to_live |string a|Indicates the maximum time period that an S3 user can specify for the 'key_time_to_live' property.

- Valid format is: 'PnDTnHnMnS\|PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds.
- If no value is specified for this property or the value specified is '0' seconds, then a user can specify any valid value.

|max_lock_retention_period |string a|Specifies the maximum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>

|metric |[metric](#) a|Performance numbers, such as IOPS latency and throughput, for SVM protocols.

|min_lock_retention_period |string a|Specifies the minimum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>

|name |string a|Specifies the name of the S3 server. A server name can contain 3 to 253 characters using only the following combination of characters:' 0-9, A-Z, a-z, ".", and "-".

|port |integer a|Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80. Valid values range from 1 to 65535.

|secure_port |integer a|Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443. Valid values range from 1 to 65535.

|statistics |[statistics](#) a|These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.

|svm |[svm](#) a|SVM, applies only to SVM-scoped objects.

|users |array[[s3_user](#)] a|This field cannot be specified in a PATCH method.

[#error_arguments] [.api-collapsible-fifth-title] error_arguments

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

code	string a	Argument code
------	----------	---------------

message	string a	Message argument
---------	----------	------------------

[#returned_error] [.api-collapsible-fifth-title] returned_error

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

arguments	array[error_arguments] a	Message arguments
-----------	--	-------------------

code	string a	Error code
------	----------	------------

message	string a	Error message
---------	----------	---------------

target	string a	The target parameter that caused the error.
--------	----------	---

=====

= Create S3 server, users, and buckets configurations

POST /protocols/s3/services

Introduced In: 9.7

Creates an S3 server, users, and buckets configurations.

== Important notes

* Each SVM can have one S3 server configuration. * One or more buckets and users can also be created using this end-point. * If creating a user configuration fails, buckets are not created either and already created users are not saved. * If creating a bucket configuration fails, all buckets already created are saved with no new buckets created.

== Required properties

* `svm.uuid` - Existing SVM in which to create an S3 server configuration.

== Recommended optional properties

* `enabled` - Specifies the state of the server created. * `comment` - Any information related to the server created.

== Default property values

* `comment` - "" * `enabled` - *true*

== Related ONTAP commands

* `vserver object-store-server create` * `vserver object-store-server bucket create` * `vserver object-store-server bucket policy statement create` * `vserver object-store-server bucket policy-statement-condition create` * `vserver object-store-server bucket cors-rule create` * `vserver object-store-server user create`

== Learn more

* [DOC /protocols/s3/services](#)

== Parameters

[cols=5*,options=header]

Name	Type	In	Required	Description
------	------	----	----------	-------------

return_records	boolean	query	False	a The default is false. If set to true, the records are returned.
----------------	---------	-------	-------	---

- Default value:

```
== Request Body
```

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

buckets	array[s3_bucket]	a This field cannot be specified in a PATCH method.
---------	------------------	---

certificate	certificate	a Specifies the certificate that will be used for creating HTTPS connections to the S3 server.
-------------	-------------	--

comment	string	a Can contain any additional information about the server being created or modified.
---------	--------	--

default_unix_user	string	a Specifies the default UNIX user for NAS Access.
-------------------	--------	---

default_win_user	string	a Specifies the default Windows user for NAS Access.
------------------	--------	--

enabled	boolean	a Specifies whether the S3 server being created or modified should be up or down.
---------	---------	---

is_http_enabled	boolean	a Specifies whether HTTP is enabled on the S3 server being created or modified. By default, HTTP is disabled on the S3 server.
-----------------	---------	--

is_https_enabled	boolean	a Specifies whether HTTPS is enabled on the S3 server being created or modified. By default, HTTPS is enabled on the S3 server.
------------------	---------	---

max_key_time_to_live	string	a Indicates the maximum time period that an S3 user can specify for the 'key_time_to_live' property.
----------------------	--------	--

- Valid format is: 'PnDTnHnMnS\|PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds.
- If no value is specified for this property or the value specified is '0' seconds, then a user can specify any valid value.

max_lock_retention_period	string	a Specifies the maximum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.
---------------------------	--------	--

min_lock_retention_period	string	a Specifies the minimum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.
---------------------------	--------	--

name	string	a Specifies the name of the S3 server. A server name can contain 3 to 253 characters using only the following combination of characters:' 0-9, A-Z, a-z, ".", and "-".
------	--------	--

port	integer	a Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80. Valid values range from 1 to 65535.
------	---------	---

secure_port	integer	a Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443. Valid values range from 1 to 65535.
-------------	---------	--

|svm |svm a|SVM, applies only to SVM-scoped objects.

|users |array[s3_user] a|This field cannot be specified in a PATCH method.

```
.Example request [%collapsible%closed] ===== [source,json,subs=+macros] { "buckets": [ { "aggregates": [ {
"name": "aggr1", "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412" } ], "audit_event_selector": { "access":
"string", "permission": "string" }, "comment": "S3 bucket.", "constituents_per_aggregate": 4, "cors": { "rules": [ {
"allowed_headers": [ "x-amz-request-id" ], "allowed_methods": [ "PUT", "DELETE" ], "allowed_origins": [
"http://www.example.com" ], "expose_headers": [ "x-amz-date" ], "id": "string", "max_age_seconds": 1024 } ] },
"lifecycle_management": { "rules": [ { "bucket_name": "bucket1", "expiration": { "object_age_days": 100,
"object_expiry_date": "2039-09-22 20:00:00 -0400" }, "name": "string", "object_filter": { "prefix": "/logs",
"size_greater_than": 10240, "size_less_than": 10485760, "tags": [ "project1=projA", "project2=projB" ] },
"svm": { "name": "svm1", "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7" }, "uuid": "414b29a1-3b26-11e9-
bd58-0050568ea055" } } ] }, "logical_used_size": 0, "name": "bucket1", "nas_path": "/", "policy": { "statements": [
{ "actions": [ "GetObject", "PutObject", "DeleteObject", "ListBucket" ], "conditions": [ { "delimiters": [ "/" ],
"max_keys": [ 1000 ], "operator": "ip_address", "prefixes": [ "pref" ], "source_ips": [ "1.1.1.1", "1.2.2.0/24" ],
"usernames": [ "user1" ] } ], "effect": "allow", "principals": [ "user1", "group/grp1", "nasgroup/group1" ],
"resources": [ "bucket1", "bucket1/" ], "sid": "FullAccessToUser1" } ] }, "qos_policy": {
"max_throughput": [ "900KB/s", "500MB/s", "120GB/s", "5000IOPS", "5000IOPS,500KB/s",
"2500IOPS,100MB/s", "1000IOPS,25MB/s" ], "max_throughput_iops": 10000,
"max_throughput_mbps": 500, "min_throughput": [ "900KB/s", "500MB/s", "120GB/s", "5000IOPS",
"5000IOPS,500KB/s", "2500IOPS,100MB/s", "1000IOPS,25MB/s" ], "min_throughput_iops": 2000,
"min_throughput_mbps": 500, "name": "performance", "uuid": "1cd8a442-86d1-11e0-ae1c-
123478563412" }, "retention": { "default_period": "P10Y", "mode": "governance" }, "role": "string",
"size": 1677721600, "snapshot_policy": { "name": "default-1weekly", "uuid": "3675af31-431c-12fa-
114a-20675afebc12" }, "storage_service_level": "value", "svm": { "name": "svm1", "uuid": "02c9e252-
41be-11e9-81d5-00a0986138f7" }, "type": "s3", "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055",
"versioning_state": "enabled", "volume": { "name": "volume1", "uuid": "028baa66-41bd-11e9-81d5-
00a0986138f7" } } ], "certificate": { "name": "string", "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}, "comment": "S3 server", "default_unix_user": "string", "default_win_user": "string",
"max_key_time_to_live": "PT6H3M", "max_lock_retention_period": "P10Y",
"min_lock_retention_period": "P10Y", "name": "Server-1", "port": 80, "secure_port": 443, "svm": {
"name": "svm1", "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7" }, "users": [ { "access_key":
"<AWS-ACCESS-KEY-ID>", "comment": "S3 user", "key_expiry_time": "2023-12-31 19:00:00 -0500",
"key_time_to_live": "PT6H3M", "name": "user-1", "secret_key": "<AWS-SECRET-ACCESS-KEY>",
"svm": { "name": "svm1", "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7" } } ] } =====
```

== Response

` Status: 201, Created `

[cols=3,options=header]

|Name |Type |Description

|num_records |integer a|Number of Records

|records |array[records] a|

```
.Example response [%collapsible%closed] ===== [source,json,subs==+macros] { "num_records": 1, "records": [
{ "job": { "uuid": "string" }, "users": [ { "access_key": "<AWS-ACCESS-KEY-ID>", "key_expiry_time": "2023-12-
31 19:00:00 -0500", "name": "user-1", "secret_key": "<AWS-SECRET-ACCESS-KEY>" } ] } ] } =====
```

```
=== Headers
```

```
[cols=3*,options=header]
```

|Name |Description |Type

|Location |Useful for tracking the resource location |string

```
== Error
```

```
` Status: Default `
```

```
ONTAP Error Response Codes [cols=2*,options=header]
```

Error Code	Description
1115127	The cluster lacks a valid S3 license.
2621706	The specified "{svm.uuid}" and "{svm.name}" refer to different SVMs.
92405789	The specified object server name contains invalid characters or not a fully qualified domain name. Valid characters for an object store server name are 0-9, A-Z, a-z, ".", and "-".
92405790	Object store server names must have between 3 and 253 characters.
92405839	Creating an object store server requires an effective cluster version of data ONTAP 9.7.0 or later. Upgrade all the nodes to 9.7.0 or later and try the operation again.
92405853	Failed to create the object store server because Cloud Volumes ONTAP does not support object store servers.
92405863	An error occurs when creating an S3 user or bucket. The reason for failure is detailed in the error message. Follow the error codes specified for the user or bucket endpoints to see details for the failure.
92405863	Failed to create bucket "{bucket name}". Reason: "Failed to create bucket "{bucket name}" for SVM "{svm.name}". Reason: Bucket name "{bucket name}" contains invalid characters or invalid character combinations. Valid characters for a bucket name are 0-9, a-z, ".", and "-". Invalid character combinations are "-.", "-.", and "-.". Resolve all the issues and retry the operation.
92405863	Failed to create bucket "{bucket name}". Reason: "Failed to create bucket "{bucket name}" for SVM "{svm.name}". Reason: Invalid QoS policy group specified "{qos policy}". The specified QoS policy group has a min-throughput value set, and the workload being assigned resides on a platform that does not support min-throughput or the cluster is in a mixed version state and the effective cluster version of ONTAP does not support min-throughput on this platform. Resolve all the issues and retry the operation.
92405863	Failed to create bucket "{bucket name}". Reason: "User(s) "{user name(s)}" specified in the principal list do not exist for SVM "{svm.name}". Use the "object-store-server user create" command to create a user.".
92405863	Failed to create user "{user name}". Reason: "SVM "Cluster" is not a data SVM. Specify a data SVM.".
92405884	An object store server can only be created on a data SVM. An object store server can also be created on a system SVM on a mixed platform cluster.
92405903	Failed to configure HTTPS on an object store server for SVM "{svm.name}". Reason: {Reason of failure}.
92405900	Certificate not found for SVM "{svm.name}".
92405917	The specified certificate name and UUID do not refer to the same certificate.
92406020	Only certificates of type "server" are supported.
92406044	Failed to set default UNIX user for SVM "{svm.name}". Reason: UNIX user can only be created on a Data SVM.
92406071	S3 protocol is not present in the allowed protocol list for SVM "{svm.name}".
92406196	The specified value for the "key_time_to_live" field cannot be greater than the maximum limit specified for the "max_key_time_to_live" field in the object store server.
92406197	Object store user "user-2" must have a non-zero value for the "key_time_to_live" field because the maximum limit specified for the "max_key_time_to_live" field in the object store server is not zero.
92406230	The value for "retention.default_period" parameter for object store bucket "<bucket>" cannot be greater than the maximum lock retention period set in the object store server for SVM "<SVM>". Check the maximum allowed lock

retention period present in the object store server for SVM "<SVM>" and try the operation again. //end row
 //start row |92406231 //end row //start row |One or more object store buckets exist with a default retention
 period greater than the "max_lock_retention_period" specified. Check the default retention period set for each
 bucket in the specified SVM and try the operation again. //end row //start row |92406236 //end row //start row
 |The value for "retention.default_period" parameter for object store bucket "<bucket>" cannot be less than the
 minimum lock retention period set in the object store server for SVM "<SVM>". Check the minimum allowed
 lock retention period present in the object store server for SVM "<SVM>" and try the operation again. //end row
 //start row |92406237 //end row //start row |One or more object store buckets exist with a default retention
 period less than the "min_lock_retention_period" specified. Check the default retention period set for each
 bucket in the specified SVM and try the operation again. //end row //start row |92406238 //end row //start row
 |The value for the "min_lock_retention_period" parameter cannot be greater than the
 "max_lock_retention_period" parameter for the object store server for SVM "vs1". //end row //start row
 |92406217 //end row //start row |The specified "-allowed-headers" in not valid because it contains more than
 one wild card ("*") character.; //end row //start row |92406224 //end row //start row |A Cross-Origin Resource
 Sharing (CORS) rule must have an origin and HTTP method specified.; //end row //start row |92406211 //end
 row //start row |The specified method "DONE" is not valid. Valid methods are GET, PUT, DELETE, HEAD, and
 POST.; //end row //start row |92405863 //end row //start row |Failed to create CORS rules for bucket "bb1".
 Reason: "Field "index" cannot be specified for this operation.". Resolve all the issues and retry the operation.;
 //end row //start row |92406228 //end row //start row |Cannot exceed the maximum limit of 100 Cross-Origin
 Resource Sharing (CORS) rules per S3 bucket "<bucket>" in SVM "<SVM>"; //end row |=== //end
 table</SVM></bucket></SVM></SVM></bucket></SVM></SVM></bucket>

Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

_links

aggregates

Aggregate

Name	Type	Description
name	string	
uuid	string	

audit_event_selector

Audit event selector allows you to specify access and permission types to audit.

Name	Type	Description
access	string	Specifies read and write access types.
permission	string	Specifies allow and deny permission types.

rules

Information about the CORS rule of an S3 bucket.

Name	Type	Description
allowed_headers	array[string]	An array of HTTP headers allowed in the cross-origin requests.
allowed_methods	array[string]	An array of HTTP methods allowed in the cross-origin requests.
allowed_origins	array[string]	List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.

Name	Type	Description
expose_headers	array[string]	List of extra headers sent in the response that customers can access from their applications.
id	string	Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
max_age_seconds	integer	The time in seconds for your browser to cache the preflight response for the specified resource.

cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
rules	array[rules]	Specifies an object store bucket CORS rule.

encryption

Name	Type	Description
enabled	boolean	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be specified in a POST method.

abort_incomplete_multipart_upload

Specifies a way to perform `abort_incomplete_multipart_upload` action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
new_non_current_versions	integer	Number of latest non-current versions to be retained.
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
prefix	string	A prefix that is matched against object-names within a bucket.
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

rules

Information about the lifecycle management rule of a bucket.

Name	Type	Description
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
bucket_name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
name	string	Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
object_filter	object_filter	Specifies a way to filter objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

Name	Type	Description
rules	array[rules]	Specifies an object store lifecycle management policy.

s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

Name	Type	Description
delimiters	array[string]	An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.
max_keys	array[integer]	An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.
operator	string	Condition operator that is applied to the specified condition key.
prefixes	array[string]	An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.

Name	Type	Description
source_ips	array[string]	An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.
usernames	array[string]	An array of usernames that a current user in the context is evaluated against using the condition operators.

s3_bucket_policy_statement

Specifies information about a single access permission.

Name	Type	Description
actions	array[string]	
conditions	array[s3_bucket_policy_condition]	Specifies bucket policy conditions.
effect	string	Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
principals	array[string]	
resources	array[string]	
sid	string	Specifies the statement identifier used to differentiate between statements. The sid length can range from 1 to 256 characters and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The

user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

Name	Type	Description
statements	array[s3_bucket_policy_statemen t]	Specifies bucket access policy statement.

destination

Name	Type	Description
is_cloud	boolean	Specifies whether a bucket is protected within the Cloud. This field cannot be specified using a POST method.
is_external_cloud	boolean	Specifies whether a bucket is protected on external Cloud providers. This field cannot be specified using a POST method.
is_ontap	boolean	Specifies whether a bucket is protected within ONTAP. This field cannot be specified using a POST method. <ul style="list-style-type: none">• Default value: 1• readOnly: 1• Introduced in: 9.10• x-nullable: true

protection_status

Specifies attributes of bucket protection.

Name	Type	Description
destination	destination	

Name	Type	Description
is_protected	boolean	<p>Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be specified using a POST method.</p> <ul style="list-style-type: none"> • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

Name	Type	Description
max_throughput	string	<p>Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.</p>
max_throughput_iops	integer	<p>Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.</p>

Name	Type	Description
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.

Name	Type	Description
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

retention

Specifies the retention mode and default retention period configured on the bucket.

Name	Type	Description
default_period	string	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.</num></num>

Name	Type	Description
mode	string	The lock mode of the bucket. compliance ‐ A SnapLock Compliance (SLC) bucket provides the highest level of WORM protection and an administrator cannot destroy a compliance bucket if it contains unexpired WORM objects. governance ‐ An administrator can delete a Governance bucket. no_lock ‐ Indicates the bucket does not support object locking.

snapshot_policy

Specifies the bucket snapshot policy.

Name	Type	Description
name	string	Specifies the name of the snapshot policy.
uuid	string	Specifies the unique identifier of the snapshot policy.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted.

Name	Type	Description
name	string	The name of the volume. This field cannot be specified in a PATCH method.
uuid	string	<p>Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move.</p> <ul style="list-style-type: none"> • example: 028baa66-41bd-11e9-81d5-00a0986138f7 • Introduced in: 9.6 • x-nullable: true

s3_bucket

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

Name	Type	Description
aggregates	array[aggregates]	A list of aggregates for FlexGroup volume constituents where the bucket is hosted. If this option is not specified, the bucket is auto-provisioned as a FlexGroup volume.
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.
audit_event_selector	audit_event_selector	Audit event selector allows you to specify access and permission types to audit.
comment	string	Can contain any additional information about the bucket being created or modified.

Name	Type	Description
constituents_per_aggregate	integer	Specifies the number of constituents or FlexVol volumes per aggregate. A FlexGroup volume consisting of all such constituents across all specified aggregates is created. This option is used along with the aggregates option and cannot be used independently.
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
is_nas_path_mutable	boolean	Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.

Name	Type	Description
lifecycle_management	lifecycle_management	Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.
name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.

Name	Type	Description
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be specified using a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
storage_service_level	string	Specifies the storage service level of the FlexGroup volume on which the bucket should be created. Valid values are "value", "performance" or "extreme".
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Specifies the bucket type. Valid values are "s3" and "nas".

Name	Type	Description
use_mirrored_aggregates	boolean	Specifies whether mirrored aggregates are selected when provisioning a FlexGroup. Only mirrored aggregates are used if this parameter is set to "true" and only unmirrored aggregates are used if this parameter is set to "false". The default value is "true" for a MetroCluster configuration and is "false" for a non-MetroCluster configuration.
uuid	string	Specifies the unique identifier of the bucket.
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted.

certificate

Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

iops

The rate of I/O operations observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency

The round trip latency in microseconds observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput

The rate of throughput bytes per second observed at the storage object.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

metric

Performance numbers, such as IOPS latency and throughput, for SVM protocols.

Name	Type	Description
duration	string	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
iops	iops	The rate of I/O operations observed at the storage object.
latency	latency	The round trip latency in microseconds observed at the storage object.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput	throughput	The rate of throughput bytes per second observed at the storage object.
timestamp	string	The timestamp of the performance data.

iops_raw

The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency_raw

The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput_raw

Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

statistics

These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.

Name	Type	Description
iops_raw	iops_raw	The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.
latency_raw	latency_raw	The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput_raw	throughput_raw	Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.
timestamp	string	The timestamp of the performance data.

s3_user

This is a container of S3 users.

Name	Type	Description
access_key	string	Specifies the access key for the user.
comment	string	Can contain any additional information about the user being created or modified.

Name	Type	Description
key_expiry_time	string	Specifies the date and time after which keys expire and are no longer valid.
key_time_to_live	string	<p>Indicates the time period from when this parameter is specified:</p> <ul style="list-style-type: none"> • when creating or modifying a user or • when the user keys were last regenerated, after which the user keys expire and are no longer valid. • Valid format is: 'PnDTnHnMnS PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If the value specified is '0' seconds, then the keys won't expire.
name	string	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".
secret_key	string	Specifies the secret key for the user.
svm	svm	SVM, applies only to SVM-scoped objects.

s3_service

Specifies the S3 server configuration.

Name	Type	Description
buckets	array[s3_bucket]	This field cannot be specified in a PATCH method.

Name	Type	Description
certificate	certificate	Specifies the certificate that will be used for creating HTTPS connections to the S3 server.
comment	string	Can contain any additional information about the server being created or modified.
default_unix_user	string	Specifies the default UNIX user for NAS Access.
default_win_user	string	Specifies the default Windows user for NAS Access.
enabled	boolean	Specifies whether the S3 server being created or modified should be up or down.
is_http_enabled	boolean	Specifies whether HTTP is enabled on the S3 server being created or modified. By default, HTTP is disabled on the S3 server.
is_https_enabled	boolean	Specifies whether HTTPS is enabled on the S3 server being created or modified. By default, HTTPS is enabled on the S3 server.
max_key_time_to_live	string	<p>Indicates the maximum time period that an S3 user can specify for the 'key_time_to_live' property.</p> <ul style="list-style-type: none"> Valid format is: 'PnDTnHnMnS PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. If no value is specified for this property or the value specified is '0' seconds, then a user can specify any valid value.

Name	Type	Description
max_lock_retention_period	string	Specifies the maximum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
min_lock_retention_period	string	Specifies the minimum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
name	string	Specifies the name of the S3 server. A server name can contain 3 to 253 characters using only the following combination of characters:' 0-9, A-Z, a-z, ".", and "-".
port	integer	Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80. Valid values range from 1 to 65535.

Name	Type	Description
secure_port	integer	Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443. Valid values range from 1 to 65535.
svm	svm	SVM, applies only to SVM-scoped objects.
users	array[s3_user]	This field cannot be specified in a PATCH method.

collection_links

job_link

Name	Type	Description
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

s3_service_user_post_response

Name	Type	Description
access_key	string	Specifies the access key for the user.
key_expiry_time	string	Specifies the date and time after which the keys expire and are no longer valid.
name	string	The name of the user.
secret_key	string	Specifies the secret key for the user.

warning

Specifies a warning message sent from the S3 server during a POST or PATCH operation.

Name	Type	Description
code	integer	Warning code of the warning encountered.

Name	Type	Description
message	string	Details of the warning sent from the S3 server.

records

Name	Type	Description
job	job_link	
users	array[s3_service_user_post_response]	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete the S3 server configuration for an SVM

```
DELETE /protocols/s3/services/{svm.uuid}
```

Introduced In: 9.7

Deletes the S3 server configuration of an SVM. If the 'delete_all' parameter is set to false, only the S3 server is deleted. Otherwise S3 users and buckets present on the SVM are also deleted. Note that only empty buckets can be deleted. This endpoint returns the S3 server delete job-uuid in response. To monitor the job status follow `/api/cluster/jobs/<job-uuid>.</job-uuid>`

Related ONTAP commands

- `vserver object-store-server delete`

Learn more

- [DOC /protocols/s3/services](#)

Parameters

Name	Type	In	Required	Description
delete_all	boolean	query	False	Delete S3 server and associated users and empty buckets. <ul style="list-style-type: none">• Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202. <ul style="list-style-type: none">• Default value: 0• Max value: 120• Min value: 0
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Response

Status: 200, Ok

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "string"
  }
}
```

Response

Status: 202, Accepted

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
92405864	An error occurs when deleting an S3 user or bucket. The reason for failure is detailed in the error message. Follow the error codes specified for the user or bucket endpoints to see details for the failure.

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

job_link

Name	Type	Description
_links	_links	
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve the S3 server configuration for an SVM

GET /protocols/s3/services/{svm.uuid}

Introduced In: 9.7

Retrieves the S3 Server configuration of an SVM. Note that in order to retrieve S3 bucket policy conditions, the 'fields' option should be set to '***'.

Related ONTAP commands

- `vserver object-store-server show`

Learn more

- [DOC /protocols/s3/services](#)

Parameters

Name	Type	In	Required	Description
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.

Response

Status: 200, Ok

Name	Type	Description
_links	self_link	
buckets	array[s3_bucket]	This field cannot be specified in a PATCH method.
certificate	certificate	Specifies the certificate that will be used for creating HTTPS connections to the S3 server.
comment	string	Can contain any additional information about the server being created or modified.
default_unix_user	string	Specifies the default UNIX user for NAS Access.
default_win_user	string	Specifies the default Windows user for NAS Access.

Name	Type	Description
enabled	boolean	Specifies whether the S3 server being created or modified should be up or down.
is_http_enabled	boolean	Specifies whether HTTP is enabled on the S3 server being created or modified. By default, HTTP is disabled on the S3 server.
is_https_enabled	boolean	Specifies whether HTTPS is enabled on the S3 server being created or modified. By default, HTTPS is enabled on the S3 server.
max_key_time_to_live	string	<p>Indicates the maximum time period that an S3 user can specify for the 'key_time_to_live' property.</p> <ul style="list-style-type: none"> Valid format is: 'PnDTnHnMnS PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. If no value is specified for this property or the value specified is '0' seconds, then a user can specify any valid value.
max_lock_retention_period	string	Specifies the maximum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
metric	metric	Performance numbers, such as IOPS latency and throughput, for SVM protocols.

Name	Type	Description
min_lock_retention_period	string	Specifies the minimum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
name	string	Specifies the name of the S3 server. A server name can contain 3 to 253 characters using only the following combination of characters:' 0-9, A-Z, a-z, ".", and "-".
port	integer	Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80. Valid values range from 1 to 65535.
secure_port	integer	Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443. Valid values range from 1 to 65535.
statistics	statistics	These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.
svm	svm	SVM, applies only to SVM-scoped objects.
users	array[s3_user]	This field cannot be specified in a PATCH method.

Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "buckets": [
    {
      "audit_event_selector": {
        "access": "string",
        "permission": "string"
      },
      "comment": "S3 bucket.",
      "cors": {
        "rules": [
          {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "allowed_headers": [
              "x-amz-request-id"
            ],
            "allowed_methods": [
              "PUT",
              "DELETE"
            ],
            "allowed_origins": [
              "http://www.example.com"
            ],
            "expose_headers": [
              "x-amz-date"
            ],
            "id": "string",
            "max_age_seconds": 1024
          }
        ]
      },
      "lifecycle_management": {
        "rules": [
          {
            "_links": {
              "self": {
```



```

        "href": "/api/resourcelink"
    }
},
"abort_incomplete_multipart_upload": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    }
},
"bucket_name": "bucket1",
"expiration": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    }
},
"object_age_days": 100,
"object_expiry_date": "2039-09-22 20:00:00 -0400"
},
"name": "string",
"non_current_version_expiration": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    }
},
"object_filter": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    }
},
"prefix": "/logs",
"size_greater_than": 10240,
"size_less_than": 10485760,
"tags": [
    "project1=projA",
    "project2=projB"
],
"svm": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    }
}

```

```

        }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
    "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055"
}
]
},
"logical_used_size": 0,
"name": "bucket1",
"nas_path": "/",
"policy": {
    "statements": [
        {
            "actions": [
                "GetObject",
                "PutObject",
                "DeleteObject",
                "ListBucket"
            ],
            "conditions": [
                {
                    "delimiters": [
                        "/"
                    ],
                    "max_keys": [
                        1000
                    ],
                    "operator": "ip_address",
                    "prefixes": [
                        "pref"
                    ],
                    "source_ips": [
                        "1.1.1.1",
                        "1.2.2.0/24"
                    ],
                    "usernames": [
                        "user1"
                    ]
                }
            ],
            "effect": "allow",
            "principals": [
                "user1",
                "group/grp1",

```

```

        "nasgroup/group1"
    ],
    "resources": [
        "bucket1",
        "bucket1/*"
    ],
    "sid": "FullAccessToUser1"
}
]
},
"qos_policy": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    },
    "max_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
    ],
    "max_throughput_iops": 10000,
    "max_throughput_mbps": 500,
    "min_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
    ],
    "min_throughput_iops": 2000,
    "min_throughput_mbps": 500,
    "name": "performance",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"retention": {
    "default_period": "P10Y",
    "mode": "governance"
},
"role": "string",

```

```

    "size": 1677721600,
    "snapshot_policy": {
      "name": "default-1weekly",
      "uuid": "3675af31-431c-12fa-114a-20675afebc12"
    },
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "type": "s3",
    "use_mirrored_aggregates": true,
    "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055",
    "versioning_state": "enabled",
    "volume": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "volume1",
      "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
    }
  },
  ],
  "certificate": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "string",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "comment": "S3 server",
  "default_unix_user": "string",
  "default_win_user": "string",
  "max_key_time_to_live": "PT6H3M",
  "max_lock_retention_period": "P10Y",
  "metric": {
    "_links": {
      "self": {

```

```

        "href": "/api/resourcelink"
    },
    },
    "duration": "PT15S",
    "iops": {
        "read": 200,
        "total": 1000,
        "write": 100
    },
    "latency": {
        "read": 200,
        "total": 1000,
        "write": 100
    },
    "status": "ok",
    "throughput": {
        "read": 200,
        "total": 1000,
        "write": 100
    },
    },
    "timestamp": "2017-01-25 06:20:13 -0500"
},
"min_lock_retention_period": "P10Y",
"name": "Server-1",
"port": 80,
"secure_port": 443,
"statistics": {
    "iops_raw": {
        "read": 200,
        "total": 1000,
        "write": 100
    },
    "latency_raw": {
        "read": 200,
        "total": 1000,
        "write": 100
    },
    },
    "status": "ok",
    "throughput_raw": {
        "read": 200,
        "total": 1000,
        "write": 100
    },
    },
    "timestamp": "2017-01-25 06:20:13 -0500"
},
"svm": {

```

```

    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "users": [
    {
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "comment": "S3 user",
      "key_expiry_time": "2023-12-31 19:00:00 -0500",
      "key_time_to_live": "PT6H3M",
      "name": "user-1",
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}

```

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

Name	Type	Description
self	href	

_links

Name	Type	Description
self	href	

aggregates

Aggregate

Name	Type	Description
_links	_links	
name	string	
uuid	string	

audit_event_selector

Audit event selector allows you to specify access and permission types to audit.

Name	Type	Description
access	string	Specifies read and write access types.
permission	string	Specifies allow and deny permission types.

rules

Information about the CORS rule of an S3 bucket.

Name	Type	Description
_links	_links	

Name	Type	Description
allowed_headers	array[string]	An array of HTTP headers allowed in the cross-origin requests.
allowed_methods	array[string]	An array of HTTP methods allowed in the cross-origin requests.
allowed_origins	array[string]	List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.
expose_headers	array[string]	List of extra headers sent in the response that customers can access from their applications.
id	string	Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
max_age_seconds	integer	The time in seconds for your browser to cache the preflight response for the specified resource.

cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
rules	array[rules]	Specifies an object store bucket CORS rule.

encryption

Name	Type	Description
enabled	boolean	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be specified in a POST method.

abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
_links	_links	
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
new_non_current_versions	integer	Number of latest non-current versions to be retained.
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
_links	_links	

Name	Type	Description
prefix	string	A prefix that is matched against object-names within a bucket.
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

rules

Information about the lifecycle management rule of a bucket.

Name	Type	Description
_links	_links	
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
bucket_name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
name	string	Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
object_filter	object_filter	Specifies a way to filter objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

Name	Type	Description
rules	array[rules]	Specifies an object store lifecycle management policy.

s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

Name	Type	Description
delimiters	array[string]	An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.
max_keys	array[integer]	An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.
operator	string	Condition operator that is applied to the specified condition key.
prefixes	array[string]	An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.
source_ips	array[string]	An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.
usernames	array[string]	An array of usernames that a current user in the context is evaluated against using the condition operators.

s3_bucket_policy_statement

Specifies information about a single access permission.

Name	Type	Description
actions	array[string]	
conditions	array[s3_bucket_policy_condition]	Specifies bucket policy conditions.

Name	Type	Description
effect	string	Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
principals	array[string]	
resources	array[string]	
sid	string	Specifies the statement identifier used to differentiate between statements. The sid length can range from 1 to 256 characters and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

Name	Type	Description
statements	array[s3_bucket_policy_statement]	Specifies bucket access policy statement.

destination

Name	Type	Description
is_cloud	boolean	Specifies whether a bucket is protected within the Cloud. This field cannot be specified using a POST method.
is_external_cloud	boolean	Specifies whether a bucket is protected on external Cloud providers. This field cannot be specified using a POST method.

Name	Type	Description
is_ontap	boolean	<p>Specifies whether a bucket is protected within ONTAP. This field cannot be specified using a POST method.</p> <ul style="list-style-type: none"> • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

protection_status

Specifies attributes of bucket protection.

Name	Type	Description
destination	destination	
is_protected	boolean	<p>Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be specified using a POST method.</p> <ul style="list-style-type: none"> • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

Name	Type	Description
_links	_links	

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

retention

Specifies the retention mode and default retention period configured on the bucket.

Name	Type	Description
default_period	string	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.</num></num>
mode	string	The lock mode of the bucket. compliance ‐ A SnapLock Compliance (SLC) bucket provides the highest level of WORM protection and an administrator cannot destroy a compliance bucket if it contains unexpired WORM objects. governance ‐ An administrator can delete a Governance bucket. no_lock ‐ Indicates the bucket does not support object locking.

snapshot_policy

Specifies the bucket snapshot policy.

Name	Type	Description
name	string	Specifies the name of the snapshot policy.
uuid	string	Specifies the unique identifier of the snapshot policy.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted.

Name	Type	Description
_links	_links	
name	string	The name of the volume. This field cannot be specified in a PATCH method.
uuid	string	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move. <ul style="list-style-type: none">• example: 028baa66-41bd-11e9-81d5-00a0986138f7• Introduced in: 9.6• x-nullable: true

s3_bucket

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.

Name	Type	Description
audit_event_selector	audit_event_selector	Audit event selector allows you to specify access and permission types to audit.
comment	string	Can contain any additional information about the bucket being created or modified.
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
is_nas_path_mutable	boolean	Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.

Name	Type	Description
lifecycle_management	lifecycle_management	Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.
name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.

Name	Type	Description
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be specified using a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Specifies the bucket type. Valid values are "s3" and "nas".
uuid	string	Specifies the unique identifier of the bucket.

Name	Type	Description
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted.

certificate

Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

Name	Type	Description
_links	_links	
name	string	Certificate name
uuid	string	Certificate UUID

iops

The rate of I/O operations observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency

The round trip latency in microseconds observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput

The rate of throughput bytes per second observed at the storage object.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

metric

Performance numbers, such as IOPS latency and throughput, for SVM protocols.

Name	Type	Description
_links	_links	
duration	string	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
iops	iops	The rate of I/O operations observed at the storage object.

Name	Type	Description
latency	latency	The round trip latency in microseconds observed at the storage object.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput	throughput	The rate of throughput bytes per second observed at the storage object.
timestamp	string	The timestamp of the performance data.

iops_raw

The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency_raw

The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput_raw

Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

statistics

These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.

Name	Type	Description
iops_raw	iops_raw	The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.
latency_raw	latency_raw	The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput_raw	throughput_raw	Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
timestamp	string	The timestamp of the performance data.

s3_user

This is a container of S3 users.

Name	Type	Description
access_key	string	Specifies the access key for the user.
comment	string	Can contain any additional information about the user being created or modified.
key_expiry_time	string	Specifies the date and time after which keys expire and are no longer valid.
key_time_to_live	string	<p>Indicates the time period from when this parameter is specified:</p> <ul style="list-style-type: none"> • when creating or modifying a user or • when the user keys were last regenerated, after which the user keys expire and are no longer valid. • Valid format is: 'PnDTnHnMnS PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If the value specified is '0' seconds, then the keys won't expire.
name	string	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".

Name	Type	Description
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update the S3 server configuration for an SVM

PATCH /protocols/s3/services/{svm.uuid}

Introduced In: 9.7

Updates the S3 Server configuration of an SVM.

Related ONTAP commands

- `vserver object-store-server modify`

Learn more

- [DOC /protocols/s3/services](#)

Parameters

Name	Type	In	Required	Description
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
certificate	certificate	Specifies the certificate that will be used for creating HTTPS connections to the S3 server.
comment	string	Can contain any additional information about the server being created or modified.
default_unix_user	string	Specifies the default UNIX user for NAS Access.
default_win_user	string	Specifies the default Windows user for NAS Access.
enabled	boolean	Specifies whether the S3 server being created or modified should be up or down.
is_http_enabled	boolean	Specifies whether HTTP is enabled on the S3 server being created or modified. By default, HTTP is disabled on the S3 server.
is_https_enabled	boolean	Specifies whether HTTPS is enabled on the S3 server being created or modified. By default, HTTPS is enabled on the S3 server.

Name	Type	Description
max_key_time_to_live	string	<p>Indicates the maximum time period that an S3 user can specify for the 'key_time_to_live' property.</p> <ul style="list-style-type: none"> Valid format is: 'PnDTnHnMnS PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. If no value is specified for this property or the value specified is '0' seconds, then a user can specify any valid value.
max_lock_retention_period	string	<p>Specifies the maximum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num></p>
min_lock_retention_period	string	<p>Specifies the minimum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num></p>

Name	Type	Description
name	string	Specifies the name of the S3 server. A server name can contain 3 to 253 characters using only the following combination of characters: '0-9, A-Z, a-z, ".", and "-'.
port	integer	Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80. Valid values range from 1 to 65535.
secure_port	integer	Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443. Valid values range from 1 to 65535.

Example request

```
{
  "certificate": {
    "name": "string",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "comment": "S3 server",
  "default_unix_user": "string",
  "default_win_user": "string",
  "max_key_time_to_live": "PT6H3M",
  "max_lock_retention_period": "P10Y",
  "min_lock_retention_period": "P10Y",
  "name": "Server-1",
  "port": 80,
  "secure_port": 443
}
```

Response

Status: 200, Ok

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
92405789	The name "{object server name}" is not valid. A valid object server name must be a fully qualified domain name.
	92405790
Object store server name is not valid. Object store server names must have between 3 and 253 characters.	
92405900	Certificate not found for SVM "{svm.name}".
	92405917
The specified certificate name and UUID do not refer to the same certificate.	
92406020	Only certificates of type "server" are supported.
	92406153
Set the enabled field of the server to "down" before modifying following fields: {field name}	
92406231	One or more object store buckets exist with a default retention period greater than the "max_lock_retention_period" specified. Check the default retention period set for each bucket in the specified SVM and try the operation again.
92406237	One or more object store buckets exist with a default retention period less than the "min_lock_retention_period" specified. Check the default retention period set for each bucket in the specified SVM and try the operation again.
92406238	The value for the "min_lock_retention_period" parameter cannot be greater than the "max_lock_retention_period" parameter for the object store server for SVM "vs1".

Definitions

See Definitions

href

Name	Type	Description
href	string	

self_link

_links

aggregates

Aggregate

Name	Type	Description
name	string	
uuid	string	

audit_event_selector

Audit event selector allows you to specify access and permission types to audit.

Name	Type	Description
access	string	Specifies read and write access types.
permission	string	Specifies allow and deny permission types.

rules

Information about the CORS rule of an S3 bucket.

Name	Type	Description
allowed_headers	array[string]	An array of HTTP headers allowed in the cross-origin requests.
allowed_methods	array[string]	An array of HTTP methods allowed in the cross-origin requests.
allowed_origins	array[string]	List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.

Name	Type	Description
expose_headers	array[string]	List of extra headers sent in the response that customers can access from their applications.
id	string	Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
max_age_seconds	integer	The time in seconds for your browser to cache the preflight response for the specified resource.

cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
rules	array[rules]	Specifies an object store bucket CORS rule.

encryption

Name	Type	Description
enabled	boolean	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be specified in a POST method.

abort_incomplete_multipart_upload

Specifies a way to perform `abort_incomplete_multipart_upload` action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
new_non_current_versions	integer	Number of latest non-current versions to be retained.
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
prefix	string	A prefix that is matched against object-names within a bucket.
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

rules

Information about the lifecycle management rule of a bucket.

Name	Type	Description
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

Name	Type	Description
rules	array[rules]	Specifies an object store lifecycle management policy.

s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

Name	Type	Description
delimiters	array[string]	An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.
max_keys	array[integer]	An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.
operator	string	Condition operator that is applied to the specified condition key.
prefixes	array[string]	An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.
source_ips	array[string]	An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.
usernames	array[string]	An array of usernames that a current user in the context is evaluated against using the condition operators.

s3_bucket_policy_statement

Specifies information about a single access permission.

Name	Type	Description
actions	array[string]	
conditions	array[s3_bucket_policy_condition]	Specifies bucket policy conditions.
effect	string	Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
principals	array[string]	
resources	array[string]	
sid	string	Specifies the statement identifier used to differentiate between statements. The sid length can range from 1 to 256 characters and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

Name	Type	Description
statements	array[s3_bucket_policy_statement]	Specifies bucket access policy statement.

destination

Name	Type	Description
is_cloud	boolean	Specifies whether a bucket is protected within the Cloud. This field cannot be specified using a POST method.

Name	Type	Description
is_external_cloud	boolean	Specifies whether a bucket is protected on external Cloud providers. This field cannot be specified using a POST method.
is_ontap	boolean	<p>Specifies whether a bucket is protected within ONTAP. This field cannot be specified using a POST method.</p> <ul style="list-style-type: none"> • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

protection_status

Specifies attributes of bucket protection.

Name	Type	Description
destination	destination	
is_protected	boolean	<p>Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be specified using a POST method.</p> <ul style="list-style-type: none"> • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

retention

Specifies the retention mode and default retention period configured on the bucket.

Name	Type	Description
default_period	string	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.</num></num>

snapshot_policy

Specifies the bucket snapshot policy.

Name	Type	Description
name	string	Specifies the name of the snapshot policy.
uuid	string	Specifies the unique identifier of the snapshot policy.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted.

Name	Type	Description
name	string	The name of the volume. This field cannot be specified in a PATCH method.
uuid	string	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move. <ul style="list-style-type: none">• example: 028baa66-41bd-11e9-81d5-00a0986138f7• Introduced in: 9.6• x-nullable: true

s3_bucket

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service. This field cannot be specified in a POST method.
audit_event_selector	audit_event_selector	Audit event selector allows you to specify access and permission types to audit.
comment	string	Can contain any additional information about the bucket being created or modified.

Name	Type	Description
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be specified using a POST or PATCH method.
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.

Name	Type	Description
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be specified using a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
type	string	Specifies the bucket type. Valid values are "s3" and "nas".
uuid	string	Specifies the unique identifier of the bucket.

Name	Type	Description
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted.

certificate

Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

iops

The rate of I/O operations observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency

The round trip latency in microseconds observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput

The rate of throughput bytes per second observed at the storage object.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

metric

Performance numbers, such as IOPS latency and throughput, for SVM protocols.

Name	Type	Description
duration	string	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
iops	iops	The rate of I/O operations observed at the storage object.

Name	Type	Description
latency	latency	The round trip latency in microseconds observed at the storage object.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput	throughput	The rate of throughput bytes per second observed at the storage object.
timestamp	string	The timestamp of the performance data.

iops_raw

The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency_raw

The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput_raw

Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

statistics

These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.

Name	Type	Description
iops_raw	iops_raw	The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.
latency_raw	latency_raw	The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput_raw	throughput_raw	Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
timestamp	string	The timestamp of the performance data.

s3_user

This is a container of S3 users.

Name	Type	Description
access_key	string	Specifies the access key for the user.
comment	string	Can contain any additional information about the user being created or modified.
key_expiry_time	string	Specifies the date and time after which keys expire and are no longer valid.
key_time_to_live	string	<p>Indicates the time period from when this parameter is specified:</p> <ul style="list-style-type: none"> • when creating or modifying a user or • when the user keys were last regenerated, after which the user keys expire and are no longer valid. • Valid format is: 'PnDTnHnMnS PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If the value specified is '0' seconds, then the keys won't expire.
secret_key	string	Specifies the secret key for the user.
svm	svm	SVM, applies only to SVM-scoped objects.

s3_service

Specifies the S3 server configuration.

Name	Type	Description
certificate	certificate	Specifies the certificate that will be used for creating HTTPS connections to the S3 server.
comment	string	Can contain any additional information about the server being created or modified.
default_unix_user	string	Specifies the default UNIX user for NAS Access.
default_win_user	string	Specifies the default Windows user for NAS Access.
enabled	boolean	Specifies whether the S3 server being created or modified should be up or down.
is_http_enabled	boolean	Specifies whether HTTP is enabled on the S3 server being created or modified. By default, HTTP is disabled on the S3 server.
is_https_enabled	boolean	Specifies whether HTTPS is enabled on the S3 server being created or modified. By default, HTTPS is enabled on the S3 server.
max_key_time_to_live	string	<p>Indicates the maximum time period that an S3 user can specify for the 'key_time_to_live' property.</p> <ul style="list-style-type: none">Valid format is: 'PnDTnHnMnS PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds.If no value is specified for this property or the value specified is '0' seconds, then a user can specify any valid value.

Name	Type	Description
max_lock_retention_period	string	Specifies the maximum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
min_lock_retention_period	string	Specifies the minimum value that can be set as the retention period for an object in a bucket with locking enabled. The value for this property can be in years or days, not both. The value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years.</num></num>
name	string	Specifies the name of the S3 server. A server name can contain 3 to 253 characters using only the following combination of characters:' 0-9, A-Z, a-z, ".", and "-".
port	integer	Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80. Valid values range from 1 to 65535.

Name	Type	Description
secure_port	integer	Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443. Valid values range from 1 to 65535.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage S3 service bucket configuration

Manage S3 service bucket configuration

Overview

An S3 bucket is a container of objects. Each bucket defines an object namespace. S3 server requests specify objects using a bucket-name and object-name pair. An object consists of data, along with optional metadata and access controls, accessible via a name. An object resides within a bucket. There can be more than one bucket in an S3 server. Buckets which are created for the server are associated with an S3 user that is created on the S3 server. An access policy is an object that when associated with a resource, defines their permissions. Buckets and objects are defined as resources. By default, only the "root" user can access these resources. Access policies are used to manage access to these resources by enabling ONTAP admin to provide "grants" to allow other users to perform operations on the buckets.

Examples

Retrieving all fields for all S3 buckets of an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-0050568ea123/buckets?fields=*&return_records=true" -H "accept: application/json"

# The response:
{
  "records": [
    {
      "svm": {
        "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
        "name": "vs1"
      },
      "uuid": "527812ab-7c6d-11e9-97e8-0050568ea123",
      "name": "bucket-2",
      "volume": {
        "name": "fg_oss_1558514455",
        "uuid": "51276f5f-7c6d-11e9-97e8-0050568ea123"
      },
      "size": 209715200,
      "logical_used_size": 157286400,
      "encryption": {
        "enabled": false
      },
      "comment": "S3 bucket.",
      "qos_policy": {
        "min_throughput_iops": 0,
        "min_throughput_mbps": 0,
        "max_throughput_iops": 1000,
        "max_throughput_mbps": 50,
        "uuid": "39ac471f-ff35-11e9-b0f9-005056a7ab52",
        "name": "vs0_auto_gen_policy_39a9522f_ff35_11e9_b0f9_005056a7ab52"
      },
      "audit_event_selector": {
        "access": "all",
        "permission": "all"
      },
      "versioning-state": "disabled",
      "snapshot-policy": {
        "name": "default-1weekly",
        "uuid": "f9c5f090-4ac8-11ef-ba24-005056a7ceb6"
      }
    }
  ]
}
```



```

    },
  },
  {
    "svm": {
      "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
      "name": "vs1"
    },
    "uuid": "a8234aec-7e06-11e9-97e8-0050568ea123",
    "name": "bucket-1",
    "volume": {
      "name": "fg_oss_1558690256",
      "uuid": "a36a1ea7-7e06-11e9-97e8-0050568ea123"
    },
    "size": 1677721600,
    "logical_used_size": 0,
    "encryption": {
      "enabled": false
    },
    "comment": "bucket1",
    "qos_policy": {
      "min_throughput_iops": 0,
      "min_throughput_mbps": 0,
      "max_throughput_iops": 1000,
      "max_throughput_mbps": 50,
      "uuid": "39ac471f-ff35-11e9-b0f9-005056a7ab52",
      "name": "vs0_auto_gen_policy_39a9522f_ff35_11e9_b0f9_005056a7ab52"
    },
    "policy": {
      "statements": [
        {
          "effect": "allow",
          "actions": [
            "*"
          ],
          "principals": [
            "Alice"
          ],
          "resources": [
            "*"
          ],
          "sid": "fullAccessForAliceToBucket"
        },
        {
          "effect": "allow",
          "actions": [
            "ListBucket",

```

```

        "GetObject"
    ],
    "principals": [
        "ann",
        "jack"
    ],
    "resources": [
        "bucket-1",
        "bucket-1/*"
    ],
    "sid": "AccessToListAndGetObjectForAnnAndJack",
    "conditions": [
        {
            "operator": "ip_address",
            "source_ips": [
                "1.1.1.1/10"
            ]
        },
        {
            "operator": "string_equals",
            "prefixes": [
                "pref1",
                "pref2"
            ],
            "usernames": [
                "user1",
                "user2"
            ],
            "delimiters": [
                "del1",
                "del2"
            ]
        },
        {
            "operator": "numeric_equals",
            "max_keys": [
                100
            ]
        }
    ]
},
{
    "effect": "deny",
    "actions": [
        "*Object"
    ],

```

```

    "principals": [
      "mike",
      "group/group1",
      "nasgroup/group2",
    ],
    "resources": [
      "bucket-1/policy-docs/*",
      "bucket-1/confidential-*"
    ],
    "sid": "DenyAccessToGetPutDeleteObjectForMike"
  },
  {
    "effect": "allow",
    "actions": [
      "GetObject"
    ],
    "principals": [
      "*"
    ],
    "resources": [
      "bucket-1/readme"
    ],
    "sid": "AccessToGetObjectForAnonymousUsers"
  },
  {
    "effect": "allow",
    "actions": [
      "GetObject"
    ],
    "principals": [
    ],
    "resources": [
      "bucket-1/policies/examples/*"
    ],
    "sid": "AccessToGetObjectForAllUsersOfSVM"
  }
]
},
"cors": {
  "rules": [
    {
      "id": "string",
      "allowed_origins": [
        "http://www.example.com"
      ],
      "allowed_methods": [

```

```
        "PUT",
        "DELETE"
    ],
    "allowed_headers": [
        "x-amz-request-id"
    ],
    "expose_headers": [
        "http://www.example.com"
    ],
    "max_age_seconds": 1024
}
]
}
}
],
"num_records": 2
}
```

Retrieving the specified bucket associated with an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{uuid}

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-0050568ea123/buckets/527812ab-7c6d-11e9-97e8-0050568ea123" -H
"accept: application/json"

# The response:
{
  "svm": {
    "uuid": "12f3ba4c-7ae0-11e9-8c06-0050568ea123",
    "name": "vs1"
  },
  "uuid": "527812ab-7c6d-11e9-97e8-0050568ea123",
  "name": "bucket-2",
  "volume": {
    "name": "fg_oss_1558514455",
    "uuid": "51276f5f-7c6d-11e9-97e8-0050568ea123"
  },
  "size": 209715200,
  "logical_used_size": 157286400,
  "encryption": {
    "enabled": false
  },
  "comment": "S3 bucket.",
  "qos_policy": {
    "min_throughput_iops": 0,
    "min_throughput_mbps": 0,
    "max_throughput_iops": 1000,
    "max_throughput_mbps": 0,
    "uuid": "39ac471f-ff35-11e9-b0f9-005056a7ab52",
    "name": "vs0_auto_gen_policy_39a9522f_ff35_11e9_b0f9_005056a7ab52"
  },
  "snapshot-policy": {
    "name": "default-1weekly",
    "uuid": "f9c5f090-4ac8-11ef-ba24-005056a7ceb6"
  },
}
```

Creating an S3 bucket for an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets

# The call:

curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-
0050568ea123/buckets?return_records=true" -H "accept: application/json" -H
"Content-Type: application/json" -d "{ \"aggregates\": [ { \"name\":
\"aggr5\", \"uuid\": \"12f3ba4c-7ae0-11e9-8c06-0050568ea123\" } ],
\"comment\": \"S3 bucket.\", \"constituents_per_aggregate\": 4, \"name\":
\"bucket-3\"}"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-
0050568ea123/buckets/?name=bucket-3
Content-Length: 353
Content-Type: application/json
{
  "num_records": 1,
  "records": [
    {
      "name": "bucket-3",
      "comment": "S3 bucket."
    }
  ],
  "job": {
    "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
      }
    }
  }
}
```

Creating an S3 bucket along with QoS policies and event selector for an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets

# The call:
curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/services/3e538980-f0af-11e9-ba68-
0050568e9798/buckets?return_records=true" -H "accept: application/json" -H
"Content-Type: application/json" -d "{ \"comment\": \"S3 bucket.\",
\"name\": \"bucket-3\", \"qos_policy\": { \"min_throughput_iops\": 0,
\"min_throughput_mbps\": 0, \"max_throughput_iops\": 1000000,
\"max_throughput_mbps\": 900000, \"uuid\": \"02d07a93-6177-11ea-b241-
000c293feac8\", \"name\":
\"vs0_auto_gen_policy_02cfa02a_6177_11ea_b241_000c293feac8\" },
\"audit_event_selector\": { \"access\": \"all\", \"permission\":
\"all\"}}}"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-
0050568ea123/buckets/?name=bucket-3
Content-Length: 353
Content-Type: application/json
{
  "num_records": 1,
  "records": [
    {
      "name": "bucket-3",
      "comment": "S3 bucket."
    }
  ],
  "job": {
    "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
      }
    }
  }
}
```

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets

# The call:

curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/services/3e538980-f0af-11e9-ba68-
0050568e9798/buckets?return_records=true" -H "accept: application/json" -H
"Content-Type: application/json" -d "{ \"aggregates\": [ { \"name\":
\"aggr5\", \"uuid\": \"12f3ba4c-7ae0-11e9-8c06-0050568ea123\" } ],
\"comment\": \"S3 bucket.\", \"constituents_per_aggregate\": 4, \"name\":
\"bucket-3\", \"policy\": { \"statements\": [ { \"actions\": [
\"GetObject\" ], \"conditions\": [ { \"operator\": \"ip_address\",
\"source_ips\": [ \"1.1.1.1/23\", \"1.2.2.2/20\" ] }, { \"max_keys\": [
1000 ], \"operator\": \"numeric_equals\" }, { \"delimiters\": [ \"/\" ],
\"operator\": \"string_equals\", \"prefixes\": [ \"pref\" ],
\"usernames\": [ \"user1\" ] } ] }, \"effect\": \"allow\", \"resources\": [
\"bucket-3/policies/examples/*\" ], \"sid\":
\"AccessToGetObjectForAllUsersofSVM\" }, { \"actions\": [ \"*Object\" ],
\"effect\": \"deny\", \"principals\": [ \"mike\", \"group/grp1\" ],
\"resources\": [ \"bucket-3/policy-docs/*\", \"bucket-3/confidential-*\"
], \"sid\": \"DenyAccessToObjectForMike\" }, { \"actions\": [
\"GetObject\" ], \"effect\": \"allow\", \"principals\": [ \"*\" ],
\"resources\": [ \"bucket-3/readme\" ], \"sid\":
\"AnonymousAccessToGetObjectForUsers\" } ] } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-
0050568ea123/buckets/?name=bucket-3
Content-Length: 353
Content-Type: application/json
{
  "num_records": 1,
  "records": [
    {
      "name": "bucket-3",
      "comment": "S3 bucket."
```



```

    }
  ],
  "job": {
    "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
      }
    }
  }
}
}

```

Creating an S3 bucket along with lifecycle management rules

```

# The API:
/api/protocols/s3/services/{svm.uuid}/buckets

# The call:

curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/services/3e538980-f0af-11e9-ba68-
0050568e9798/buckets?return_records=true" -H "accept: application/json" -H
"Content-Type: application/json" -d "{ \"aggregates\": [ { \"name\":
\"aggr5\", \"uuid\": \"12f3ba4c-7ae0-11e9-8c06-0050568ea123\" } ],
\"comment\": \"S3 bucket.\", \"constituents_per_aggregate\": 4, \"name\":
\"bucket-4\", \"lifecycle_management\": { \"rules\": [ { \"name\":
\"rule1\", \"expiration\": { \"object_age_days\" : \"1000\" } ,
\"abort_incomplete_multipart_upload\" : { \"after_initiation_days\" : 200
} , \"object_filter\": { \"prefix\" : \"obj1*/\" , \"size_greater_than\"
: \"1000\" } } , { \"name\": \"rule2\", \"object_filter\": {
\"size_greater_than\" : \"50\" } , \"expiration\": { \"object_age_days\" :
\"5000\" } } ] } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 18 April 2022 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-
0050568ea123/buckets/?name=bucket-4
Content-Length: 363
Content-Type: application/json

```

```
{
  "num_records": 1,
  "records": [
    {
      "name": "bucket-4",
      "comment": "S3 bucket."
    }
  ],
  "job": {
    "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
      }
    }
  }
}
```

Creating an S3 bucket with object locking enabled for an SVM

```

# The API:
/api/protocols/s3/services/{svm.uuid}/buckets

# The call:

curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-
0050568ea143/buckets?return_records=true" -H "accept: application/json" -H
"Content-Type: application/json" -d "{ \"aggregates\": [ { \"name\":
\"aggr5\", \"uuid\": \"12f3ba4c-7ae0-11e9-8c06-0050568ea143\" } ],
\"comment\": \"S3 Compliance mode bucket.\",
\"constituents_per_aggregate\": 4, \"name\": \"bucket-5\", \"retention\":
{ \"mode\": \"compliance\", \"default_period\" : \"P1Y\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2023 11:25:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-
0050568ea143/buckets/?name=bucket-5
Content-Length: 353
Content-Type: application/json
{
  "num_records": 1,
  "records": [
    {
      "name": "bucket-5",
      "comment": "S3 Compliance mode bucket."
    }
  ],
  "job": {
    "uuid": "2e880171-7e16-11e9-bfdc-0050568ea143",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea143"
      }
    }
  }
}

```

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/s3/services/2da46d66-2327-11ef-ab73-005056a7a2dd/buckets?return_timeout=0&return_records=true" -H
"accept: application/json" -H "authorization: Basic <CREDENTIALS>" -H
"Content-Type: application/json" -d "{ \"cors\": { \"rules\": [{
  \"allowed_headers\": [ \"x-amz-request-id\" ], \"allowed_methods\": [
  \"PUT\", \"DELETE\" ], \"allowed_origins\": [ \"http://www.example.com\"
  ], \"expose_headers\": [ \"http://www.example.com\" ], \"id\": \"id1\",
  \"max_age_seconds\": 1024 }]}, \"name\": \"bucket1\"}"

# The response:
HTTP/1.1 202 Accepted
Date: Thu, 06 Jun 2024 09:18:26 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-
inline'; style-src 'self' 'unsafe-inline'; img-src 'self' data;; frame-
ancestors: 'self'
Location: /api/protocols/s3/services/2da46d66-2327-11ef-ab73-
005056a7a2dd/buckets/baf69601-23e5-11ef-ab73-005056a7a2dd
Content-Length: 871
Content-Type: application/json
Vary: Origin
{
  "num_records": 1,
  "records": [
    {
      "uuid": "baf69601-23e5-11ef-ab73-005056a7a2dd",
      "name": "bucket1",
      "type": "s3",
      "cors": {
        "rules": [
          {
            "id": "id1",
            "allowed_origins": [
              "http://www.example.com"
            ],
            "allowed_methods": [
              "PUT",
              "DELETE"
            ]
          }
        ]
      }
    }
  ]
}
```

```

    ],
    "allowed_headers": [
        "x-amz-request-id"
    ],
    "expose_headers": [
        "http://www.example.com"
    ],
    "max_age_seconds": 1024
  }
]
}
},
"job": {
  "uuid": "baf69953-23e5-11ef-ab73-005056a7a2dd",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/baf69953-23e5-11ef-ab73-005056a7a2dd"
    }
  }
}
}
}

```

Creating an S3 bucket with a snapshot-policy

```

# The API:
/api/protocols/s3/services/{svm.uuid}/buckets

# The call:
curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-
0050568ea143/buckets?return_records=true" -H "accept: application/json" -H
"Content-Type: application/json" -d "{ \"comment\": \"S3 snapshot policy
bucket.\", \"snapshot_policy\": { \"name\": \"default-1weekly\", \"uuid\":
\"f9c5f090-4ac8-11ef-ba24-005056a7ceb6\" }, \"name\": \"bucket-6\" }"

# The response:
HTTP/1.1 202 Accepted
Date: Thu, 25 Jul 2024 16:40:37 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/8c38f10b-4871-11ef-aab5-
005056a7ceb6/buckets/9f21f404-4aa4-11ef-ba24-005056a7ceb6
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "9f21f716-4aa4-11ef-ba24-005056a7ceb6",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/9f21f716-4aa4-11ef-ba24-005056a7ceb6"
      }
    }
  }
}

```

Updating an S3 bucket for an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-0050568ea123/buckets/754389d0-7e13-11e9-bfdc-0050568ea122" -H "accept: application/json?return_records=true" -H "Content-Type: application/json" -d "{ \"comment\": \"Bucket modified.\", \"size\": 11111111111, \"qos_policy\": { \"min_throughput_iops\": 0, \"min_throughput_mbps\": 0, \"max_throughput_iops\": 1000000, \"max_throughput_mbps\": 900000, \"uuid\": \"02d07a93-6177-11ea-b241-000c293feac8\", \"name\": \"vs0_auto_gen_policy_02cfa02a_6177_11ea_b241_000c293feac8\"}}}"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "9beafabb-7e17-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/9beafabb-7e17-11e9-bfdc-0050568ea123"
      }
    }
  }
}
```

Updating an S3 bucket policy and event selector for an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/3e538980-f0af-11e9-ba68-0050568e9798/buckets/754389d0-7e13-11e9-bfdc-0050568ea122?return_records=true" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"policy\": { \"statements\": [ { \"actions\": [ \"*\"] , \"conditions\": [ { \"operator\": \"ip_address\", \"source_ips\": [ \"1.1.1.1/23\", \"1.2.2.2/20\" ] }, { \"max_keys\": [ 1000 ], \"operator\": \"numeric_equals\" }, { \"delimiters\": [ \"/\" ], \"operator\": \"string_equals\", \"prefixes\": [ \"pref\" ], \"usernames\": [ \"user1\" ] } ] , \"effect\": \"allow\", \"resources\": [ \"*\"] , \"sid\": \"fullAccessForAllPrincipalsToBucket\" } ] }, \"audit_event_selector\": { \"access\": \"read\", \"permission\": \"deny\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "9beafabb-7e17-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/9beafabb-7e17-11e9-bfdc-0050568ea123"
      }
    }
  }
}
```

Updating the default-retention period on an S3 bucket for an SVM


```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/3e538980-f0af-11e9-ba68-0050568e9798/buckets/754389d0-7e13-11e9-bfdc-0050568ea122?return_records=true" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"retention\": { \"default_period\": \"P10Y\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2023 11:35:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "9beafabb-7e17-11e9-bfdc-0050568ea143",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/9beafabb-7e17-11e9-bfdc-0050568ea143"
      }
    }
  }
}
```

Updating the CORS rules of an S3 bucket for an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/2da46d66-2327-11ef-ab73-005056a7a2dd/buckets/dce4e40-2330-11ef-ab73-005056a7a2dd?return_timeout=0" -H "accept: application/json" -H "authorization: Basic <CREDENTIALS>" -H "Content-Type: application/json" -d "{ \"cors\": { \"rules\": [{ \"allowed_headers\": [ \"x-amz-new-header\" ], \"allowed_methods\": [ \"PUT\" ], \"allowed_origins\": [ \"http://www.example.in\" ], \"expose_headers\": [ \"http://www.example\" ], \"id\": \"id3\", \"max_age_seconds\": 10 } ] } }"

# The response:
HTTP/1.1 202 Accepted
Date: Thu, 06 Jun 2024 09:30:57 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self' data:; frame-ancestors: 'self'
Content-Length: 189
Content-Type: application/json
Vary: Origin
{
  "job": {
    "uuid": "7aaa2b64-23e7-11ef-ab73-005056a7a2dd",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/7aaa2b64-23e7-11ef-ab73-005056a7a2dd"
      }
    }
  }
}
```

Updating the snapshot-policy for an S3 bucket for an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/3e538980-f0af-11e9-ba68-0050568e9798/buckets/754389d0-7e13-11e9-bfdc-0050568ea122?return_records=true" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"snapshot_policy\": { \"name\": \"default-1weekly\", \"uuid\": \"f9c5f090-4ac8-11ef-ba24-005056a7ceb6\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Thu, 25 Jul 2024 16:56:44 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "df350023-4aa6-11ef-ba24-005056a7ceb6",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/df350023-4aa6-11ef-ba24-005056a7ceb6"
      }
    }
  }
}
```

Deleting an S3 bucket policy for an SVM

```

# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/3e538980-f0af-11e9-ba68-0050568e9798/buckets/754389d0-7e13-11e9-bfdc-0050568ea122?return_records=true" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"policy\": { \"statements\": [ ] } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "9beafabb-7e17-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/9beafabb-7e17-11e9-bfdc-0050568ea123"
      }
    }
  }
}

```

Deleting CORS rules for an S3 bucket in an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/3e538980-f0af-11e9-ba68-0050568e9798/buckets/754389d0-7e13-11e9-bfdc-0050568ea122?return_records=true" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"cors\": { \"rules\": [ ] } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2024 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "9beafabb-7e17-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/9beafabb-7e17-11e9-bfdc-0050568ea123"
      }
    }
  }
}
```

Deleting an S3 bucket for a specified SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{uuid}

# The call:
curl -iku admin:<password> -X DELETE "https://<mgmt-
ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-
0050568ea123/buckets/754389d0-7e13-11e9-bfdc-
0050568ea123?return_records=true" -H "accept: application/json"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 24 May 2019 11:40:17 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
{
  "job": {
    "uuid": "b3af4a54-7e18-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/b3af4a54-7e18-11e9-bfdc-0050568ea123"
      }
    }
  }
}
```

Retrieve the S3 bucket configurations for an SVM

GET /protocols/s3/services/{svm.uuid}/buckets

Introduced In: 9.7

Retrieves the S3 bucket's configuration of an SVM. Note that in order to retrieve S3 bucket policy conditions, the 'fields' option should be set to '***'.

Related ONTAP commands

- vserver object-store-server bucket show
- vserver object-store-server bucket policy statement show
- vserver object-store-server bucket policy-statement-condition show
- vserver object-store-server bucket lifecycle-management-rule show

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/buckets](#)

Parameters

Name	Type	In	Required	Description
lifecycle_management.rules.uuid	string	query	False	Filter by lifecycle_management.rules.uuid <ul style="list-style-type: none">• Introduced in: 9.14
lifecycle_management.rules.name	string	query	False	Filter by lifecycle_management.rules.name <ul style="list-style-type: none">• Introduced in: 9.13• maxLength: 256• minLength: 0
lifecycle_management.rules.bucket_name	string	query	False	Filter by lifecycle_management.rules.bucket_name <ul style="list-style-type: none">• Introduced in: 9.14• maxLength: 63• minLength: 3
lifecycle_management.rules.non_current_version_expiration.new_non_current_versions	integer	query	False	Filter by lifecycle_management.rules.non_current_version_expiration.new_non_current_versions <ul style="list-style-type: none">• Introduced in: 9.13

Name	Type	In	Required	Description
lifecycle_management.rules.non_current_version_expiration.non_current_days	integer	query	False	Filter by lifecycle_management.rules.non_current_version_expiration.non_current_days • Introduced in: 9.13
lifecycle_management.rules.expiration.object_age_days	integer	query	False	Filter by lifecycle_management.rules.expiration.object_age_days • Introduced in: 9.13
lifecycle_management.rules.expiration.expired_object_delete_marker	boolean	query	False	Filter by lifecycle_management.rules.expiration.expired_object_delete_marker • Introduced in: 9.13
lifecycle_management.rules.expiration.object_expiry_date	string	query	False	Filter by lifecycle_management.rules.expiration.object_expiry_date • Introduced in: 9.13
lifecycle_management.rules.object_filter.tags	string	query	False	Filter by lifecycle_management.rules.object_filter.tags • Introduced in: 9.13
lifecycle_management.rules.object_filter.prefix	string	query	False	Filter by lifecycle_management.rules.object_filter.prefix • Introduced in: 9.13

Name	Type	In	Required	Description
lifecycle_management.rules.object_filter.size_greater_than	integer	query	False	Filter by lifecycle_management.rules.object_filter.size_greater_than • Introduced in: 9.13
lifecycle_management.rules.object_filter.size_less_than	integer	query	False	Filter by lifecycle_management.rules.object_filter.size_less_than • Introduced in: 9.13
lifecycle_management.rules.enabled	boolean	query	False	Filter by lifecycle_management.rules.enabled • Introduced in: 9.13
lifecycle_management.rules.abort_incomplete_multipart_upload.after_initiation_days	integer	query	False	Filter by lifecycle_management.rules.abort_incomplete_multipart_upload.after_initiation_days • Introduced in: 9.13
lifecycle_management.rules.svm.name	string	query	False	Filter by lifecycle_management.rules.svm.name • Introduced in: 9.14
lifecycle_management.rules.svm.uuid	string	query	False	Filter by lifecycle_management.rules.svm.uuid • Introduced in: 9.14
svm.name	string	query	False	Filter by svm.name

Name	Type	In	Required	Description
encryption.enabled	boolean	query	False	Filter by encryption.enabled
comment	string	query	False	Filter by comment <ul style="list-style-type: none"> • maxLength: 256 • minLength: 0
size	integer	query	False	Filter by size <ul style="list-style-type: none"> • Max value: 62672162783232000 • Min value: 199229440
role	string	query	False	Filter by role <ul style="list-style-type: none"> • Introduced in: 9.10
qos_policy.min_throughput_mbps	integer	query	False	Filter by qos_policy.min_throughput_mbps <ul style="list-style-type: none"> • Introduced in: 9.8 • Max value: 4194303 • Min value: 0
qos_policy.max_throughput_mbps	integer	query	False	Filter by qos_policy.max_throughput_mbps <ul style="list-style-type: none"> • Introduced in: 9.8 • Max value: 4194303 • Min value: 0
qos_policy.name	string	query	False	Filter by qos_policy.name <ul style="list-style-type: none"> • Introduced in: 9.8

Name	Type	In	Required	Description
qos_policy.uuid	string	query	False	Filter by qos_policy.uuid <ul style="list-style-type: none"> Introduced in: 9.8
qos_policy.max_throughput	string	query	False	Filter by qos_policy.max_throughput <ul style="list-style-type: none"> Introduced in: 9.17
qos_policy.max_throughput_iops	integer	query	False	Filter by qos_policy.max_throughput_iops <ul style="list-style-type: none"> Introduced in: 9.8 Max value: 2147483647 Min value: 0
qos_policy.min_throughput_iops	integer	query	False	Filter by qos_policy.min_throughput_iops <ul style="list-style-type: none"> Introduced in: 9.8 Max value: 2147483647 Min value: 0
qos_policy.min_throughput	string	query	False	Filter by qos_policy.min_throughput <ul style="list-style-type: none"> Introduced in: 9.17
policy.statements.resources	string	query	False	Filter by policy.statements.resources <ul style="list-style-type: none"> Introduced in: 9.8

Name	Type	In	Required	Description
policy.statements.actions	string	query	False	Filter by policy.statements.actions • Introduced in: 9.8
policy.statements.effect	string	query	False	Filter by policy.statements.effect • Introduced in: 9.8
policy.statements.conditions.usernames	string	query	False	Filter by policy.statements.conditions.usernames • Introduced in: 9.8
policy.statements.conditions.source_ips	string	query	False	Filter by policy.statements.conditions.source_ips • Introduced in: 9.8
policy.statements.conditions.max_keys	integer	query	False	Filter by policy.statements.conditions.max_keys • Introduced in: 9.8
policy.statements.conditions.delimiters	string	query	False	Filter by policy.statements.conditions.delimiters • Introduced in: 9.8
policy.statements.conditions.operator	string	query	False	Filter by policy.statements.conditions.operator • Introduced in: 9.8

Name	Type	In	Required	Description
policy.statements.conditions.prefixes	string	query	False	Filter by policy.statements.conditions.prefixes <ul style="list-style-type: none"> Introduced in: 9.8
policy.statements.principals	string	query	False	Filter by policy.statements.principals <ul style="list-style-type: none"> Introduced in: 9.8
policy.statements.sid	string	query	False	Filter by policy.statements.sid <ul style="list-style-type: none"> Introduced in: 9.8 maxLength: 256 minLength: 0
logical_used_size	integer	query	False	Filter by logical_used_size
is_nas_path_mutable	boolean	query	False	Filter by is_nas_path_mutable <ul style="list-style-type: none"> Introduced in: 9.17
uuid	string	query	False	Filter by uuid
retention.mode	string	query	False	Filter by retention.mode <ul style="list-style-type: none"> Introduced in: 9.14
retention.default_period	string	query	False	Filter by retention.default_period <ul style="list-style-type: none"> Introduced in: 9.14

Name	Type	In	Required	Description
nas_path	string	query	False	Filter by nas_path <ul style="list-style-type: none"> Introduced in: 9.12
cors.rules.expose_headers	string	query	False	Filter by cors.rules.expose_headers <ul style="list-style-type: none"> Introduced in: 9.16
cors.rules.max_age_seconds	integer	query	False	Filter by cors.rules.max_age_seconds <ul style="list-style-type: none"> Introduced in: 9.16
cors.rules.allowed_origins	string	query	False	Filter by cors.rules.allowed_origins <ul style="list-style-type: none"> Introduced in: 9.16
cors.rules.allowed_methods	string	query	False	Filter by cors.rules.allowed_methods <ul style="list-style-type: none"> Introduced in: 9.16
cors.rules.allowed_headers	string	query	False	Filter by cors.rules.allowed_headers <ul style="list-style-type: none"> Introduced in: 9.16
cors.rules.id	string	query	False	Filter by cors.rules.id <ul style="list-style-type: none"> Introduced in: 9.16 maxLength: 256 minLength: 0

Name	Type	In	Required	Description
versioning_state	string	query	False	Filter by versioning_state <ul style="list-style-type: none"> • Introduced in: 9.11
audit_event_selector.permission	string	query	False	Filter by audit_event_selector.permission <ul style="list-style-type: none"> • Introduced in: 9.10
audit_event_selector.access	string	query	False	Filter by audit_event_selector.access <ul style="list-style-type: none"> • Introduced in: 9.10
protection_status.is_protected	boolean	query	False	Filter by protection_status.is_protected <ul style="list-style-type: none"> • Introduced in: 9.10
protection_status.destination.is_ontap	boolean	query	False	Filter by protection_status.destination.is_ontap <ul style="list-style-type: none"> • Introduced in: 9.10
protection_status.destination.is_cloud	boolean	query	False	Filter by protection_status.destination.is_cloud <ul style="list-style-type: none"> • Introduced in: 9.10
protection_status.destination.is_external_cloud	boolean	query	False	Filter by protection_status.destination.is_external_cloud <ul style="list-style-type: none"> • Introduced in: 9.12

Name	Type	In	Required	Description
snapshot_policy.uuid	string	query	False	Filter by snapshot_policy.uuid • Introduced in: 9.16
snapshot_policy.name	string	query	False	Filter by snapshot_policy.name • Introduced in: 9.16
volume.uuid	string	query	False	Filter by volume.uuid
volume.name	string	query	False	Filter by volume.name
type	string	query	False	Filter by type • Introduced in: 9.12
is_consistent_etag	boolean	query	False	Filter by is_consistent_etag • Introduced in: 9.17
name	string	query	False	Filter by name • maxLength: 63 • minLength: 3
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Max value: 120 • Min value: 0 • Default value: 15
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

Status: 200, Ok

Name	Type	Description
_links	collection_links	
num_records	integer	Number of records
records	array[s3_bucket_svm]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "audit_event_selector": {
        "access": "string",
        "permission": "string"
      },
      "comment": "S3 bucket.",
      "cors": {
        "rules": [
          {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "allowed_headers": [
              "x-amz-request-id"
            ],
            "allowed_methods": [
              "PUT",
              "DELETE"
            ],
            "allowed_origins": [
              "http://www.example.com"
            ],
            "expose_headers": [
              "x-amz-date"
            ],
            "id": "string",
            "max_age_seconds": 1024
          }
        ]
      },
      "lifecycle_management": {
```

```

"rules": [
  {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "abort_incomplete_multipart_upload": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    },
    "bucket_name": "bucket1",
    "expiration": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    },
    "object_age_days": 100,
    "object_expiry_date": "2039-09-22 20:00:00 -0400"
  },
  "name": "string",
  "non_current_version_expiration": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "object_filter": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "prefix": "/logs",
  "size_greater_than": 10240,
  "size_less_than": 10485760,
  "tags": [
    "project1=projA",
    "project2=projB"
  ]
},

```

```

        "svm": {
            "_links": {
                "self": {
                    "href": "/api/resourcelink"
                }
            },
            "name": "svm1",
            "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
        },
        "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055"
    ]
}
},
"logical_used_size": 0,
"name": "bucket1",
"nas_path": "/",
"policy": {
    "statements": [
        {
            "actions": [
                "GetObject",
                "PutObject",
                "DeleteObject",
                "ListBucket"
            ],
            "conditions": [
                {
                    "delimiters": [
                        "/"
                    ],
                    "max_keys": [
                        1000
                    ],
                    "operator": "ip_address",
                    "prefixes": [
                        "pref"
                    ],
                    "source_ips": [
                        "1.1.1.1",
                        "1.2.2.0/24"
                    ],
                    "usernames": [
                        "user1"
                    ]
                }
            ]
        }
    ],

```

```

        "effect": "allow",
        "principals": [
            "user1",
            "group/grp1",
            "nasgroup/group1"
        ],
        "resources": [
            "bucket1",
            "bucket1/*"
        ],
        "sid": "FullAccessToUser1"
    }
]
},
"qos_policy": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    },
    "max_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
    ],
    "max_throughput_iops": 10000,
    "max_throughput_mbps": 500,
    "min_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
    ],
    "min_throughput_iops": 2000,
    "min_throughput_mbps": 500,
    "name": "performance",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"retention": {

```

```

    "default_period": "P10Y",
    "mode": "governance"
  },
  "role": "string",
  "size": 819200000,
  "snapshot_policy": {
    "name": "default-1weekly",
    "uuid": "3675af31-431c-12fa-114a-20675afebc12"
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "type": "s3",
  "uuid": "string",
  "versioning_state": "enabled",
  "volume": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "volume1",
    "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
  }
}
]
}

```

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

collection_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

aggregates

Aggregate

Name	Type	Description
_links	_links	
name	string	
uuid	string	

audit_event_selector

Event selector allows you to specify access and permission types to audit.

Name	Type	Description
access	string	Specifies read and write access types.
permission	string	Specifies allow and deny permission types.

rules

Information about the CORS rule of an S3 bucket.

Name	Type	Description
_links	_links	

Name	Type	Description
allowed_headers	array[string]	An array of HTTP headers allowed in the cross-origin requests.
allowed_methods	array[string]	An array of HTTP methods allowed in the cross-origin requests.
allowed_origins	array[string]	List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.
expose_headers	array[string]	List of extra headers sent in the response that customers can access from their applications.
id	string	Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
max_age_seconds	integer	The time in seconds for your browser to cache the preflight response for the specified resource.

cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
rules	array[rules]	Specifies an object store bucket CORS rule.

encryption

Name	Type	Description
enabled	boolean	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be set in a POST or PATCH method.

abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
_links	_links	
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
new_non_current_versions	integer	Number of latest non-current versions to be retained.
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
_links	_links	

Name	Type	Description
prefix	string	A prefix that is matched against object-names within a bucket.
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

rules

Information about the lifecycle management rule of a bucket.

Name	Type	Description
_links	_links	
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
bucket_name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
name	string	Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
object_filter	object_filter	Specifies a way to filter objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

Name	Type	Description
rules	array[rules]	Specifies an object store lifecycle management policy. This field cannot be set using the PATCH method.

s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

Name	Type	Description
delimiters	array[string]	An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.
max_keys	array[integer]	An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.
operator	string	Condition operator that is applied to the specified condition key.
prefixes	array[string]	An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.
source_ips	array[string]	An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.
usernames	array[string]	An array of usernames that a current user in the context is evaluated against using the condition operators.

s3_bucket_policy_statement

Specifies information about a single access permission.

Name	Type	Description
actions	array[string]	
conditions	array[s3_bucket_policy_condition]	Specifies bucket policy conditions.

Name	Type	Description
effect	string	Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
principals	array[string]	
resources	array[string]	
sid	string	Specifies the statement identifier used to differentiate between statements. The sid length can range from 1 to 256 characters and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

Name	Type	Description
statements	array[s3_bucket_policy_statement]	Specifies bucket access policy statement.

destination

Name	Type	Description
is_cloud	boolean	Specifies whether a bucket is protected within the Cloud.
is_external_cloud	boolean	Specifies whether a bucket is protected on external Cloud providers.

Name	Type	Description
is_ontap	boolean	<p>Specifies whether a bucket is protected within ONTAP.</p> <ul style="list-style-type: none"> • Default value: • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

protection_status

Specifies attributes of bucket protection.

Name	Type	Description
destination	destination	
is_protected	boolean	<p>Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be set in a POST method.</p> <ul style="list-style-type: none"> • Default value: • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

Name	Type	Description
_links	_links	

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

retention

Specifies the retention mode and default retention period configured on the bucket.

Name	Type	Description
default_period	string	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.</num></num>
mode	string	The lock mode of the bucket. compliance ‐ A SnapLock Compliance (SLC) bucket provides the highest level of WORM protection and an administrator cannot destroy a compliance bucket if it contains unexpired WORM objects. governance ‐ An administrator can delete a Governance bucket. no_lock ‐ Indicates the bucket does not support object locking.

snapshot_policy

Specifies the bucket snapshot policy.

Name	Type	Description
name	string	Specifies the name of the snapshot policy.
uuid	string	Specifies the unique identifier of the snapshot policy.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted. This field cannot be set in a POST method.

Name	Type	Description
_links	_links	
name	string	The name of the volume. This field cannot be specified in a PATCH method.
uuid	string	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move. <ul style="list-style-type: none">• example: 028baa66-41bd-11e9-81d5-00a0986138f7• Introduced in: 9.6• x-nullable: true

s3_bucket_svm

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

Name	Type	Description
audit_event_selector	audit_event_selector	Event selector allows you to specify access and permission types to audit.

Name	Type	Description
comment	string	Can contain any additional information about the bucket being created or modified.
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
is_nas_path_mutable	boolean	Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.

Name	Type	Description
lifecycle_management	lifecycle_management	Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be set using the PATCH method.
name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.

Name	Type	Description
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be set in a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Specifies the bucket type. Valid values are "s3" and "nas". This field cannot be set using the PATCH method.
uuid	string	Specifies the unique identifier of the bucket. This field cannot be specified in a POST or PATCH method.

Name	Type	Description
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted. This field cannot be set in a POST method.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create an S3 bucket configuration for an SVM

POST /protocols/s3/services/{svm.uuid}/buckets

Introduced In: 9.7

Creates the S3 bucket configuration of an SVM.

Important notes

- Each SVM can have one or more bucket configurations.
- Aggregate lists should be specified explicitly. If not specified, then the bucket is auto-provisioned as a

FlexGroup.

- Constituents per aggregate specifies the number of components (or FlexVols) per aggregate. Is specified only when an aggregate list is explicitly defined.
- An access policy can be created when a bucket is created.
- "qos_policy" can be specified if a bucket needs to be attached to a QoS group policy during creation time.
- "audit_event_selector" can be specified if a bucket needs to be specify access and permission type for auditing.
- Cross-origin resource sharing (CORS) configuration can be specified when a bucket is created.

Required properties

- `svm.uuid` - Existing SVM in which to create the bucket configuration.
- `name` - Bucket name that is to be created.

Recommended optional properties

- `aggregates` - List of aggregates for the FlexGroup on which the bucket is hosted on.
- `constituents_per_aggregate` - Number of constituents per aggregate.
- `size` - Specifying the bucket size is recommended.
- `policy` - Specifying policy enables users to perform operations on buckets; specifying the resource permissions is recommended.
- `qos_policy` - A QoS policy for buckets.
- `audit_event_selector` - Audit policy for buckets.
- `versioning_state` - Versioning state for buckets.
- `type` - Type of bucket.
- `nas_path` - The NAS path to which the NAS bucket corresponds to.
- `use_mirrored_aggregates` - Specifies whether mirrored aggregates are selected when provisioning a FlexGroup volume.
- `lifecycle_management` - Object store server lifecycle management policy.
- `retention.mode` - Object lock mode supported on the bucket.
- `retention.default_period` - Specifies the duration of default-retention applicable for objects on the object store bucket.
- `cors` - Specifying CORS rules enables the bucket to service the cross-origin requests.
- `snapshot_policy` - Snapshot policy for the bucket.
- `is_consistent_etag` - Return a consistent ETag for NAS buckets.
- `is_nas_path_mutable` - Specifies whether the NAS bucket mapping with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount.

Default property values

- `size` - 800MB
- `comment` - ""
- `aggregates` - No default value.
- `constituents_per_aggregate` - 4 , if an aggregates list is specified. Otherwise, no default value.
- `policy.statements.actions` - `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `ListBucketMultipartUploads`, `ListMultipartUploadParts`, `GetObjectTagging`, `PutObjectTagging`, `DeleteObjectTagging`, `GetBucketVersioning`, `PutBucketVersioning`.
- `policy.statements.principals` - all S3 users and groups in the SVM or the NAS groups.
- `policy.statements.resources` - all objects in the bucket.
- `policy.statements.conditions` - list of bucket policy conditions.
- `qos-policy` - No default value.
- `versioning_state` - disabled.
- `use_mirrored_aggregates` - *true* for a MetroCluster configuration and *false* for a non-MetroCluster configuration.
- `type` - S3.
- `retention.mode` - `no_lock`
- `is_consistent_etag` - `false`

Related ONTAP commands

- `vserver object-store-server bucket create`
- `vserver object-store-server bucket policy statement create`
- `vserver object-store-server bucket policy-statement-condition create`
- `vserver object-store-server bucket lifecycle-management-rule create`
- `vserver object-store-server bucket cors-rule create`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/buckets](#)

Parameters

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none"> • Default value: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	<p>The default is false. If set to true, the records are returned.</p> <ul style="list-style-type: none"> • Default value:
svm.uuid	string	path	True	<p>UUID of the SVM to which this object belongs.</p>

Request Body

Name	Type	Description
aggregates	array[aggregates]	A list of aggregates for FlexGroup volume constituents where the bucket is hosted. If this option is not specified, the bucket is auto-provisioned as a FlexGroup volume. The "uuid" field cannot be used with the field "storage_service_level".
audit_event_selector	audit_event_selector	Event selector allows you to specify access and permission types to audit.
comment	string	Can contain any additional information about the bucket being created or modified.
constituents_per_aggregate	integer	Specifies the number of constituents or FlexVol volumes per aggregate. A FlexGroup volume consisting of all such constituents across all specified aggregates is created. This option is used along with the aggregates option and cannot be used independently. This field cannot be set using the PATCH method.
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.

Name	Type	Description
is_nas_path_mutable	boolean	Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.
lifecycle_management	lifecycle_management	Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be set using the PATCH method.
name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.

Name	Type	Description
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps" . Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be set in a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 190MB to 62PB.
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.

Name	Type	Description
storage_service_level	string	Specifies the storage service level of the FlexGroup volume on which the bucket should be created. Valid values are "value", "performance" or "extreme". This field cannot be used with the field "aggregates.uuid" or with the "constituents_per_aggregate" in a POST method. This field cannot be set using the PATCH method.
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Specifies the bucket type. Valid values are "s3" and "nas". This field cannot be set using the PATCH method.
uuid	string	Specifies the unique identifier of the bucket. This field cannot be specified in a POST or PATCH method.
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted. This field cannot be set in a POST method.

Example request

```
{
  "aggregates": [
    {
      "name": "aggr1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ],
  "audit_event_selector": {
    "access": "string",
    "permission": "string"
  },
  "comment": "S3 bucket.",
  "constituents_per_aggregate": 4,
  "cors": {
    "rules": [
      {
        "allowed_headers": [
          "x-amz-request-id"
        ],
        "allowed_methods": [
          "PUT",
          "DELETE"
        ],
        "allowed_origins": [
          "http://www.example.com"
        ],
        "expose_headers": [
          "x-amz-date"
        ],
        "id": "string",
        "max_age_seconds": 1024
      }
    ]
  },
  "lifecycle_management": {
    "rules": [
      {
        "bucket_name": "bucket1",
        "expiration": {
          "object_age_days": 100,
          "object_expiry_date": "2039-09-22 20:00:00 -0400"
        },
        "name": "string",
        "object_filter": {
```

```

        "prefix": "/logs",
        "size_greater_than": 10240,
        "size_less_than": 10485760,
        "tags": [
            "project1=projA",
            "project2=projB"
        ]
    },
    "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055"
}
]
},
"logical_used_size": 0,
"name": "bucket1",
"nas_path": "/",
"policy": {
    "statements": [
        {
            "actions": [
                "GetObject",
                "PutObject",
                "DeleteObject",
                "ListBucket"
            ],
            "conditions": [
                {
                    "delimiters": [
                        "/"
                    ],
                    "max_keys": [
                        1000
                    ],
                    "operator": "ip_address",
                    "prefixes": [
                        "pref"
                    ],
                    "source_ips": [
                        "1.1.1.1",
                        "1.2.2.0/24"
                    ],
                    "usernames": [
                        "user1"
                    ]
                }
            ]
        }
    ]
}

```



```

        ]
    },
    "effect": "allow",
    "principals": [
        "user1",
        "group/grp1",
        "nasgroup/group1"
    ],
    "resources": [
        "bucket1",
        "bucket1/*"
    ],
    "sid": "FullAccessToUser1"
}
],
},
"qos_policy": {
    "max_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
    ],
    "max_throughput_iops": 10000,
    "max_throughput_mbps": 500,
    "min_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
    ],
    "min_throughput_iops": 2000,
    "min_throughput_mbps": 500,
    "name": "performance",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"retention": {
    "default_period": "P10Y",
    "mode": "governance"
}
}

```

```

},
"role": "string",
"size": 819200000,
"snapshot_policy": {
  "name": "default-1weekly",
  "uuid": "3675af31-431c-12fa-114a-20675afebc12"
},
"storage_service_level": "value",
"svm": {
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"type": "s3",
"uuid": "string",
"versioning_state": "enabled",
"volume": {
  "name": "volume1",
  "uuid": "028baa66-41bd-11e9-81d5-00a0986138f7"
}
}

```

Response

Status: 202, Accepted

Name	Type	Description
job	job_link	

Example response

```

{
  "job": {
    "uuid": "string"
  }
}

```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Response

Status: 201, Created

Error

Status: Default

ONTAP Error Response Codes

Error code	Message
92405777	"Failed to create bucket "{bucket name}" for SVM "{svm.name}". Reason: {Reason of failure}.";
92405785	"Bucket name "{bucket name}" contains invalid characters or invalid character combinations. Valid characters for a bucket name are 0-9, a-z, ".", and "-". Invalid character combinations are "-.", "-.", and "..".";
92405786	"Bucket name "{bucket name}" is not valid. Bucket names must have between 3 and 63 characters. ";
92405811	"Failed to create bucket "{bucket name}" for SVM "{svm.name}". Wait a few minutes and try the operation again.";
92405812	"Failed to create the object store volume. Reason: {Reason for failure}.";
92405819	"Cannot provision an object store server volume for bucket "{bucket name}" in SVM "{svm.name}" on the following aggregates because they are SnapLock aggregates: {List of aggregates.name}.";
92405820	"Failed to check whether the aggregate "{aggregates.name}" is a FabricPool. Reason: {Reason for failure}.";
92405821	"Cannot provision an object store server volume for bucket "{bucket name}" in SVM "{svm.name}" on the following aggregates because they are FabricPool: {List of aggregates.name}.";
92405827	"Internal Error. Unable to generate object store volume name.";
92405857	"One or more aggregates must be specified if "constituents_per_aggregate" is specified.";
92405858	"Failed to "create" the "bucket" because the operation is only supported on data SVMs.";
92405859	"The specified "aggregates.uuid" "{aggregates.uuid}" does not exist.";

Error code	Message
92405860	"The specified "aggregates.name" "{aggregates.name}" and "aggregates.uuid" "{aggregates.uuid}" do not refer to same aggregate.";
92405861	"The specified SVM UUID or bucket UUID does not exist.";
92405863	"Failed to create access policies for bucket "{bucket name}". Reason: {Reason of Failure}. Resolve all the issues and retry the operation.";
92405863	"Failed to create event selector for bucket "{bucket name}". Reason: {Reason of failure}. Reason: object-store-server audit configuration not created for SVM "{svm.name}". Resolve all the issues and retry the operation.";
92405891	The resources specified in the access policy are not valid. Valid ways to specify a resource are *, <bucket-name>, <bucket-name>/.../.... Valid characters for a resource are 0-9, A-Z, a-z, _, +, comma, ;, :, =, ., &, @, ?, (,), single quote, *, !, - and \$.
92406166	"Cannot enable locking on a NAS bucket.";
92406170	"Cannot set "-default-retention-period" on object store bucket "{0}" in Vserver "{1}". Setting the default retention period on an object store bucket requires an effective cluster version of 9.14.1 or later.";
92406171	"Cannot set "{retention_mode}" to "compliance" in a MetroCluster configuration";
92406174	"Internal error. Failed to complete bucket create workflow with "-retention-mode" set to "compliance" or "governance". Reason: {0}";
92406175	"The SnapLock compliance clock is not running. Use the "snaplock compliance-clock initialize" command to initialize the compliance clock, and then try the operation again.";
92406176	"The SnapLock compliance clock is not running on the MetroCluster partner cluster. Use the "snaplock compliance-clock initialize" command to initialize the compliance clock on the MetroCluster partner cluster, and then try the operation again.";
92406230	"The value for "retention.default_period" parameter for object store bucket "<bucket>" cannot be greater than the maximum lock retention period set in the object store server for SVM "<SVM>". Check the maximum allowed lock retention period present in the object store server for SVM "<SVM>" and try the operation again."; //end row //start row

Error code	Message
92406236 //end row //start row	"The value for "retention.default_period" parameter for object store bucket "<bucket>" cannot be less than the minimum lock retention period set in the object store server for SVM "<SVM>". Check the minimum allowed lock retention period present in the object store server for SVM "<SVM>" and try the operation again."; //end row //start row
92406217 //end row //start row	"The specified "allowed_headers" is not valid because it contains more than one wild card ("*") character."; //end row //start row
92406224 //end row //start row	"A Cross-Origin Resource Sharing (CORS) rule must have an origin and HTTP method specified."; //end row //start row
92406222 //end row //start row	"Cannot specify Cross-Origin Resource Sharing (CORS) configuration for object store bucket "<bucket>" on SVM "<SVM>". Specifying such configuration is supported on object store volumes created in ONTAP 9.8 or later releases only."; //end row //start row
92406211 //end row //start row	"The specified method "DONE" is not valid. Valid methods are GET, PUT, DELETE, HEAD, and POST."; //end row //start row
92405863 //end row //start row	"Failed to create CORS rules for bucket "bb1". Reason: "Field "index" cannot be specified for this operation.". Resolve all the issues and retry the operation."; //end row //start row
92406228 //end row //start row	"Cannot exceed the maximum limit of 100 Cross-Origin Resource Sharing (CORS) rules per S3 bucket "<bucket>" in SVM "<SVM>".;"; //end row

|Name |Type |Description

|href |string a|

[#_links] [.api-collapsible-fifth-title] _links [#aggregates] [.api-collapsible-fifth-title] aggregates
Aggregate
[cols=3*,options=header]

|Name |Type |Description

|name |string a|

|uuid |string a|

[#audit_event_selector] [.api-collapsible-fifth-title] audit_event_selector

Event selector allows you to specify access and permission types to audit.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

access	string a	Specifies read and write access types.
--------	----------	--

permission	string a	Specifies allow and deny permission types.
------------	----------	--

[#rules] [.api-collapsible-fifth-title] rules

Information about the CORS rule of an S3 bucket.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

allowed_headers	array[string] a	An array of HTTP headers allowed in the cross-origin requests.
-----------------	-----------------	--

allowed_methods	array[string] a	An array of HTTP methods allowed in the cross-origin requests.
-----------------	-----------------	--

allowed_origins	array[string] a	List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.
-----------------	-----------------	---

expose_headers	array[string] a	List of extra headers sent in the response that customers can access from their applications.
----------------	-----------------	---

id	string a	Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
----	----------	---

max_age_seconds	integer a	The time in seconds for your browser to cache the preflight response for the specified resource.
-----------------	-----------	--

[#cors] [.api-collapsible-fifth-title] cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

rules	array[rules] a	Specifies an object store bucket CORS rule.
-------	----------------------------------	---

[#encryption] [.api-collapsible-fifth-title] encryption

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

enabled	boolean a	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be set in a POST or PATCH method.
---------	-----------	--

#abort_incomplete_multipart_upload [.api-collapsible-fifth-title] abort_incomplete_multipart_upload		
---	--	--

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

[cols=3*,options=header]		
--------------------------	--	--

Name	Type	Description
------	------	-------------

after_initiation_days	integer a	Number of days of initiation after which uploads can be aborted.
-----------------------	-----------	--

#expiration [.api-collapsible-fifth-title] expiration		
---	--	--

Specifies a way to perform expiration action on filtered objects within a bucket.

[cols=3*,options=header]		
--------------------------	--	--

Name	Type	Description
------	------	-------------

expired_object_delete_marker	boolean a	Cleanup object delete markers.
------------------------------	-----------	--------------------------------

object_age_days	integer a	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
-----------------	-----------	--

object_expiry_date	string a	Specific date from when objects can expire. This cannot be used with object_age_days.
--------------------	----------	---

#non_current_version_expiration [.api-collapsible-fifth-title] non_current_version_expiration		
---	--	--

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

[cols=3*,options=header]		
--------------------------	--	--

Name	Type	Description
------	------	-------------

new_non_current_versions	integer a	Number of latest non-current versions to be retained.
--------------------------	-----------	---

non_current_days	integer a	Number of days after which non-current versions can be deleted.
------------------	-----------	---

#object_filter [.api-collapsible-fifth-title] object_filter		
---	--	--

Specifies a way to filter objects within a bucket.

[cols=3*,options=header]		
--------------------------	--	--

Name	Type	Description
------	------	-------------

prefix	string a	A prefix that is matched against object-names within a bucket.
--------	----------	--

|size_greater_than |integer a|Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.

|size_less_than |integer a|Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.

|tags |array[string] a|An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

```
[#svm] [.api-collapsible-fifth-title] svm
```

Specifies the name of the SVM where this bucket exists.

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

name	string a	The name of the SVM. This field cannot be specified in a PATCH method.
------	----------	--

uuid	string a	The unique identifier of the SVM. This field cannot be specified in a PATCH method.
------	----------	---

```
[#rules] [.api-collapsible-fifth-title] rules
```

Information about the lifecycle management rule of a bucket.

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

abort_incomplete_multipart_upload	abort_incomplete_multipart_upload a	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
-----------------------------------	---	--

bucket_name	string a	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
-------------	----------	--

enabled	boolean a	Specifies whether or not the associated rule is enabled.
---------	-----------	--

expiration	expiration a	Specifies a way to perform expiration action on filtered objects within a bucket.
------------	------------------------------	---

name	string a	Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.
------	----------	---

non_current_version_expiration	non_current_version_expiration a	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
--------------------------------	--	---

object_filter	object_filter a	Specifies a way to filter objects within a bucket.
---------------	---------------------------------	--

svm	svm a	Specifies the name of the SVM where this bucket exists.
-----	-----------------------	---

uuid	string a	Specifies the unique identifier of the bucket.
------	----------	--

[#lifecycle_management] [.api-collapsible-fifth-title] lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

rules	array[rules]	a Specifies an object store lifecycle management policy. This field cannot be set using the PATCH method.
-------	--------------------------------	---

[#s3_bucket_policy_condition] [.api-collapsible-fifth-title] s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

delimiters	array[string]	a An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.
------------	---------------	--

max_keys	array[integer]	a An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.
----------	----------------	--

operator	string	a Condition operator that is applied to the specified condition key.
----------	--------	--

prefixes	array[string]	a An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.
----------	---------------	---

source_ips	array[string]	a An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.
------------	---------------	--

usernames	array[string]	a An array of usernames that a current user in the context is evaluated against using the condition operators.
-----------	---------------	--

[#s3_bucket_policy_statement] [.api-collapsible-fifth-title] s3_bucket_policy_statement

Specifies information about a single access permission.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

actions	array[string]	a
---------	---------------	---

conditions	array[s3_bucket_policy_condition]	a Specifies bucket policy conditions.
------------	---	---------------------------------------

effect	string	a Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
--------	--------	--

|principals |array[string] a|

|resources |array[string] a|

|sid |string a|Specifies the statement identifier used to differentiate between statements. The sid length can range from 1 to 256 characters and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

[#policy] [.api-collapsible-fifth-title] policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

[cols=3*,options=header]

|Name |Type |Description

|statements |array[s3_bucket_policy_statement] a|Specifies bucket access policy statement.

[#destination] [.api-collapsible-fifth-title] destination

[cols=3*,options=header]

|Name |Type |Description

|is_cloud |boolean a|Specifies whether a bucket is protected within the Cloud.

|is_external_cloud |boolean a|Specifies whether a bucket is protected on external Cloud providers.

|is_ontap |boolean a|Specifies whether a bucket is protected within ONTAP.

- Default value: 1
- readOnly: 1
- Introduced in: 9.10
- x-nullable: true

[#protection_status] [.api-collapsible-fifth-title] protection_status

Specifies attributes of bucket protection.

[cols=3*,options=header]

|Name |Type |Description

|destination |destination a|

|is_protected |boolean a|Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be set in a POST method.

- Default value: 1

- readOnly: 1
- Introduced in: 9.10
- x-nullable: true

```
[#qos_policy] [.api-collapsible-fifth-title] qos_policy
```

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

max_throughput	string a	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
----------------	----------	---

max_throughput_iops	integer a	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
---------------------	-----------	--

max_throughput_mbps	integer a	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
---------------------	-----------	---

min_throughput	string a	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
----------------	----------	--

min_throughput_iops	integer a	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
---------------------	-----------	---

min_throughput_mbps	integer a	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
---------------------	-----------	---

name	string a	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
------	----------	---

uuid	string a	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.
------	----------	---

[#retention] [.api-collapsible-fifth-title] retention

Specifies the retention mode and default retention period configured on the bucket.

[cols=3*,options=header]

|Name |Type |Description

|default_period |string a|Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.</num></num>

|mode |string a|The lock mode of the bucket. compliance ‐ A SnapLock Compliance (SLC) bucket provides the highest level of WORM protection and an administrator cannot destroy a compliance bucket if it contains unexpired WORM objects. governance ‐ An administrator can delete a Governance bucket. no_lock ‐ Indicates the bucket does not support object locking.

[#snapshot_policy] [.api-collapsible-fifth-title] snapshot_policy

Specifies the bucket snapshot policy.

[cols=3*,options=header]

|Name |Type |Description

|name |string a|Specifies the name of the snapshot policy.

|uuid |string a|Specifies the unique identifier of the snapshot policy.

[#svm] [.api-collapsible-fifth-title] svm

SVM, applies only to SVM-scoped objects.

[cols=3*,options=header]

|Name |Type |Description

|name |string a|The name of the SVM. This field cannot be specified in a PATCH method.

|uuid |string a|The unique identifier of the SVM. This field cannot be specified in a PATCH method.

[#volume] [.api-collapsible-fifth-title] volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted. This field cannot be set in a POST method.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

name	string a	The name of the volume. This field cannot be specified in a PATCH method.
------	----------	---

uuid	string a	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move.
------	----------	---

- example: 028baa66-41bd-11e9-81d5-00a0986138f7
- Introduced in: 9.6
- x-nullable: true

```
[#s3_bucket_svm] [.api-collapsible-fifth-title] s3_bucket_svm
```

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

aggregates	array[aggregates] a	A list of aggregates for FlexGroup volume constituents where the bucket is hosted. If this option is not specified, the bucket is auto-provisioned as a FlexGroup volume. The "uuid" field cannot be used with the field "storage_service_level".
------------	---------------------------------------	---

audit_event_selector	audit_event_selector a	Event selector allows you to specify access and permission types to audit.
----------------------	--	--

comment	string a	Can contain any additional information about the bucket being created or modified.
---------	----------	--

constituents_per_aggregate	integer a	Specifies the number of constituents or FlexVol volumes per aggregate. A FlexGroup volume consisting of all such constituents across all specified aggregates is created. This option is used along with the aggregates option and cannot be used independently. This field cannot be set using the PATCH method.
----------------------------	-----------	---

cors	cors a	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
------	------------------------	---

encryption	encryption a	
------------	------------------------------	--

is_consistent_etag	boolean a	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
--------------------	-----------	--

is_nas_path_mutable	boolean a	Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.
---------------------	-----------	--

lifecycle_management	lifecycle_management a	Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied
----------------------	--	--

in the background and can delete objects.

|logical_used_size |integer a|Specifies the bucket logical used size up to this point. This field cannot be set using the PATCH method.

|name |string a|Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".

|nas_path |string a|Specifies the NAS path to which the nas bucket corresponds to.

|policy |[policy](#) a|A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

|protection_status |[protection_status](#) a|Specifies attributes of bucket protection.

|qos_policy |[qos_policy](#) a|Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

|retention |[retention](#) a|Specifies the retention mode and default retention period configured on the bucket.

|role |string a|Specifies the role of the bucket. This field cannot be set in a POST method.

|size |integer a|Specifies the bucket size in bytes; ranges from 190MB to 62PB.

|snapshot_policy |[snapshot_policy](#) a|Specifies the bucket snapshot policy.

|storage_service_level |string a|Specifies the storage service level of the FlexGroup volume on which the bucket should be created. Valid values are "value", "performance" or "extreme". This field cannot be used with the field "aggregates.uuid" or with the "constituents_per_aggregate" in a POST method. This field cannot be set using the PATCH method.

|svm |[svm](#) a|SVM, applies only to SVM-scoped objects.

|type |string a|Specifies the bucket type. Valid values are "s3" and "nas". This field cannot be set using the PATCH method.

|uuid |string a|Specifies the unique identifier of the bucket. This field cannot be specified in a POST or PATCH method.

|versioning_state |string a|Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.

|volume |[volume](#) a|Specifies the FlexGroup volume name and UUID where the bucket is hosted. This field cannot be set in a POST method.

```
[#job_link] [.api-collapsible-fifth-title] job_link
```

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

uuid	string a	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.
------	----------	---

[#error_arguments] [.api-collapsible-fifth-title] error_arguments

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

code	string a	Argument code
------	----------	---------------

message	string a	Message argument
---------	----------	------------------

[#returned_error] [.api-collapsible-fifth-title] returned_error

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

arguments	array[error_arguments] a	Message arguments
-----------	--	-------------------

code	string a	Error code
------	----------	------------

message	string a	Error message
---------	----------	---------------

target	string a	The target parameter that caused the error.
--------	----------	---

====

= Delete an S3 bucket configuration for an SVM

DELETE /protocols/s3/services/{svm.uuid}/buckets/{uuid}

Introduced In: 9.7

Deletes the S3 bucket configuration of an SVM. An access policy is also deleted on an S3 bucket "delete" command. All CORS rules are also deleted on bucket deletion.

== Related ONTAP commands

* vserver object-store-server bucket delete * vserver object-store-server bucket policy statement delete * vserver object-store-server bucket policy-statement-condition delete * vserver object-store-server bucket lifecycle-management-rule delete * vserver object-store-server bucket cors-rule delete

== Learn more

* [DOC /protocols/s3/services/{svm.uuid}/buckets](#)

== Parameters

[cols=5*,options=header]

Name	Type	In	Required	Description
------	------	----	----------	-------------

uuid	string	path	True	a The unique identifier of the bucket.
------	--------	------	------	--

return_timeout	integer	query	False	a The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.
----------------	---------	-------	-------	--

- Default value: 0
- Max value: 120
- Min value: 0

svm.uuid	string	path	True	a UUID of the SVM to which this object belongs.
----------	--------	------	------	---

== Response

```
` Status: 200, Ok `
```

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

job	job_link	a
-----	--------------------------	---

.Example response [%collapsible%closed] ===== [source,json,subs=+macros] { "job": { "_links": { "self": { "href": "/api/resourcelink" } }, "uuid": "string" } } =====

== Response

```
` Status: 202, Accepted `
```

== Error

```
` Status: Default `
```

ONTAP Error Response Codes [cols=2*,options=header]

Error code	Message
------------	---------

92405811	"Failed to delete bucket "{bucket name}" for SVM "{svm.name}". Wait a few minutes and try the operation again."; 92405858
----------	--

92405861	"Failed to "delete" the "bucket" because the operation is only supported on data SVMs."; 92405779
----------	--

92405813	"The specified SVM UUID or bucket UUID does not exist."; 92405864
----------	--

92405864	"Failed to remove bucket "{bucket name}" for SVM "{svm.name}". Reason: {Reason for failure}."; 92405864
----------	--

92405864	"Failed to delete the object store volume. Reason: {Reason for failure}."; 92405864
----------	--

92405864	"An error occurred when deleting an access policy. The reason for failure is detailed in the error message."; 92405864
----------	---

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

|error |[returned_error](#) a|

```
.Example error [%collapsible%closed] ==== [source,json,subs=+macros] { "error": { "arguments": [ { "code":  
"string", "message": "string" } ], "code": "4", "message": "entry doesn't exist", "target": "uuid" } } =====
```

== Definitions

[.api-def-first-level] .See Definitions [%collapsible%closed] ===== [[#href](#)] [.api-collapsible-fifth-title] href

[cols=3*,options=header]

|Name |Type |Description

|href |string a|

[[#_links](#)] [.api-collapsible-fifth-title] _links

[cols=3*,options=header]

|Name |Type |Description

|self |[href](#) a|

[[#job_link](#)] [.api-collapsible-fifth-title] job_link

[cols=3*,options=header]

|Name |Type |Description

|_links |[_links](#) a|

|uuid |string a|The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

[[#error_arguments](#)] [.api-collapsible-fifth-title] error_arguments

[cols=3*,options=header]

|Name |Type |Description

|code |string a|Argument code

|message |string a|Message argument

[[#returned_error](#)] [.api-collapsible-fifth-title] returned_error

[cols=3*,options=header]

|Name |Type |Description

|arguments |array[[error_arguments](#)] a|Message arguments

|code |string a|Error code

|message |string a|Error message

|target |string a|The target parameter that caused the error.

====

= Retrieve an S3 bucket for an SVM

GET /protocols/s3/services/{svm.uuid}/buckets/{uuid}

Introduced In: 9.7

Retrieves the S3 bucket configuration of an SVM. Note that in order to retrieve S3 bucket policy conditions, the 'fields' option should be set to '*'.

== Related ONTAP commands

* vservers object-store-server bucket show * vservers object-store-server bucket policy statement show * vservers object-store-server bucket policy-statement-condition show * vservers object-store-server bucket lifecycle-management-rule show * vservers object-store-server bucket cors-rule show

== Learn more

* [DOC /protocols/s3/services/{svm.uuid}/buckets](#)

== Parameters

[cols=5,options=header]

Name	Type	In	Required	Description
------	------	----	----------	-------------

uuid	string path	True	a	The unique identifier of the bucket.
------	--------------	------	---	--------------------------------------

svm.uuid	string path	True	a	UUID of the SVM to which this object belongs.
----------	--------------	------	---	---

fields	array string	query	False	a Specify the fields to return.
--------	--------------	-------	-------	---------------------------------

== Response

` Status: 200, Ok `

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

audit_event_selector	audit_event_selector	a Event selector allows you to specify access and permission types to audit.
----------------------	--------------------------------------	--

comment	string	a Can contain any additional information about the bucket being created or modified.
---------	--------	--

cors	cors	a Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an
------	----------------------	---

origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

|encryption |[encryption](#) a|

|is_consistent_etag |boolean a|Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.

|is_nas_path_mutable |boolean a|Specifies whether the NAS bucket mapping or association with a NAS volume can change according to the changes in the NAS volume junction-path due to volume operations like mount and unmount and therefore the NAS bucket will have access to any path in a NAS volume that matches the specified nas-path. Or is immutable and therefore the NAS bucket will always have access to the same nas-path that was specified during bucket creation even if the volume junction-path has undergone changes after the bucket creation.

|lifecycle_management |[lifecycle_management](#) a|Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

|logical_used_size |integer a|Specifies the bucket logical used size up to this point. This field cannot be set using the PATCH method.

|name |string a|Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".

|nas_path |string a|Specifies the NAS path to which the nas bucket corresponds to.

|policy |[policy](#) a|A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

|protection_status |[protection_status](#) a|Specifies attributes of bucket protection.

|qos_policy |[qos_policy](#) a|Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

|retention |[retention](#) a|Specifies the retention mode and default retention period configured on the bucket.

|role |string a|Specifies the role of the bucket. This field cannot be set in a POST method.

|size |integer a|Specifies the bucket size in bytes; ranges from 190MB to 62PB.

|snapshot_policy |[snapshot_policy](#) a|Specifies the bucket snapshot policy.

|svm |[svm](#) a|SVM, applies only to SVM-scoped objects.

|type |string a|Specifies the bucket type. Valid values are "s3" and "nas". This field cannot be set using the PATCH method.

|uuid |string a|Specifies the unique identifier of the bucket. This field cannot be specified in a POST or PATCH

method.

|versioning_state |string a|Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.

|volume |volume a|Specifies the FlexGroup volume name and UUID where the bucket is hosted. This field cannot be set in a POST method.

```
.Example response [%collapsible%closed] ==== [source,json,subs==+macros] { "audit_event_selector": {
"access": "string", "permission": "string" }, "comment": "S3 bucket.", "cors": { "rules": [ { "_links": { "self": {
"href": "/api/resourcelink" } } }, "allowed_headers": [ "x-amz-request-id" ], "allowed_methods": [ "PUT",
"DELETE" ], "allowed_origins": [ "http://www.example.com" ], "expose_headers": [ "x-amz-date" ], "id": "string",
"max_age_seconds": 1024 } } }, "lifecycle_management": { "rules": [ { "_links": { "self": { "href":
"/api/resourcelink" } } }, "abort_incomplete_multipart_upload": { "_links": { "self": { "href": "/api/resourcelink" } } },
"bucket_name": "bucket1", "expiration": { "_links": { "self": { "href": "/api/resourcelink" } } }, "object_age_days":
100, "object_expiry_date": "2039-09-22 20:00:00 -0400" }, "name": "string", "non_current_version_expiration":
{ "_links": { "self": { "href": "/api/resourcelink" } } }, "object_filter": { "_links": { "self": { "href": "/api/resourcelink" }
} }, "prefix": "/logs", "size_greater_than": 10240, "size_less_than": 10485760, "tags": [ "project1=projA",
"project2=projB" ] }, "svm": { "_links": { "self": { "href": "/api/resourcelink" } } }, "name": "svm1", "uuid":
"02c9e252-41be-11e9-81d5-00a0986138f7" }, "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055" } ] },
"logical_used_size": 0, "name": "bucket1", "nas_path": "/", "policy": { "statements": [ { "actions": [ "GetObject",
"PutObject", "DeleteObject", "ListBucket" ], "conditions": [ { "delimiters": [ "/" ], "max_keys": [ 1000 ], "operator":
"ip_address", "prefixes": [ "pref" ], "source_ips": [ "1.1.1.1", "1.2.2.0/24" ], "usernames": [ "user1" ] } ], "effect":
"allow", "principals": [ "user1", "group/grp1", "nasgroup/group1" ], "resources": [ "bucket1", "bucket1/" ], "sid":
"FullAccessToUser1" } ] }, "qos_policy": { "_links": { "self": { "href": "/api/resourcelink" } } },
"max_throughput": [ "900KB/s", "500MB/s", "120GB/s", "5000IOPS", "5000IOPS,500KB/s",
"2500IOPS,100MB/s", "1000IOPS,25MB/s" ], "max_throughput_iops": 10000,
"max_throughput_mbps": 500, "min_throughput": [ "900KB/s", "500MB/s", "120GB/s", "5000IOPS",
"5000IOPS,500KB/s", "2500IOPS,100MB/s", "1000IOPS,25MB/s" ], "min_throughput_iops": 2000,
"min_throughput_mbps": 500, "name": "performance", "uuid": "1cd8a442-86d1-11e0-ae1c-
123478563412" }, "retention": { "default_period": "P10Y", "mode": "governance" }, "role": "string",
"size": 819200000, "snapshot_policy": { "name": "default-1weekly", "uuid": "3675af31-431c-12fa-114a-
20675afebc12" }, "svm": { "_links": { "self": { "href": "/api/resourcelink" } } }, "name": "svm1", "uuid":
"02c9e252-41be-11e9-81d5-00a0986138f7" }, "type": "s3", "uuid": "string", "versioning_state":
"enabled", "volume": { "_links": { "self": { "href": "/api/resourcelink" } } }, "name": "volume1", "uuid":
"028baa66-41bd-11e9-81d5-00a0986138f7" } } =====
```

== Error

` Status: Default, Error `

[cols=3,options=header]

|Name |Type |Description

|error |returned_error a|

.Example error [%collapsible%closed] ==== [source,json,subs=+macros] { "error": { "arguments": [{ "code": "string", "message": "string" }], "code": "4", "message": "entry doesn't exist", "target": "uuid" } } ====

== Definitions

[.api-def-first-level] .See Definitions [%collapsible%closed] ==== [#href] [.api-collapsible-fifth-title] href

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

href	string a	
------	----------	--

[#_links] [.api-collapsible-fifth-title] _links

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

self	href a	
------	------------------------	--

[#aggregates] [.api-collapsible-fifth-title] aggregates

Aggregate

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links a	
--------	--------------------------	--

name	string a	
------	----------	--

uuid	string a	
------	----------	--

[#audit_event_selector] [.api-collapsible-fifth-title] audit_event_selector

Event selector allows you to specify access and permission types to audit.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

access	string a	Specifies read and write access types.
--------	----------	--

permission	string a	Specifies allow and deny permission types.
------------	----------	--

[#rules] [.api-collapsible-fifth-title] rules

Information about the CORS rule of an S3 bucket.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

<code>_links</code>	links	a
---------------------	-----------------------	---

<code>allowed_headers</code>	<code>array[string]</code>	aAn array of HTTP headers allowed in the cross-origin requests.
------------------------------	----------------------------	---

<code>allowed_methods</code>	<code>array[string]</code>	aAn array of HTTP methods allowed in the cross-origin requests.
------------------------------	----------------------------	---

<code>allowed_origins</code>	<code>array[string]</code>	aList of origins from where a cross-origin request is allowed to originate from for the S3 bucket.
------------------------------	----------------------------	--

<code>expose_headers</code>	<code>array[string]</code>	aList of extra headers sent in the response that customers can access from their applications.
-----------------------------	----------------------------	--

<code>id</code>	<code>string</code>	aBucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
-----------------	---------------------	--

<code>max_age_seconds</code>	<code>integer</code>	aThe time in seconds for your browser to cache the preflight response for the specified resource.
------------------------------	----------------------	---

[#cors] [.api-collapsible-fifth-title] cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

<code>rules</code>	<code>array[rules]</code>	aSpecifies an object store bucket CORS rule.
--------------------	---	--

[#encryption] [.api-collapsible-fifth-title] encryption

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

<code>enabled</code>	<code>boolean</code>	aSpecifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be set in a POST or PATCH method.
----------------------	----------------------	---

[#abort_incomplete_multipart_upload] [.api-collapsible-fifth-title] abort_incomplete_multipart_upload

Specifies a way to perform `abort_incomplete_multipart_upload` action on filtered objects within a bucket. It cannot be specified with tags.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

<code>_links</code>	links	a
---------------------	-----------------------	---

|after_initiation_days |integer a|Number of days of initiation after which uploads can be aborted.

[#expiration] [.api-collapsible-fifth-title] expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

[cols=3*,options=header]

|Name |Type |Description

|_links |[_links](#) a|

|expired_object_delete_marker |boolean a|Cleanup object delete markers.

|object_age_days |integer a|Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.

|object_expiry_date |string a|Specific date from when objects can expire. This cannot be used with object_age_days.

[#non_current_version_expiration] [.api-collapsible-fifth-title] non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

[cols=3*,options=header]

|Name |Type |Description

|_links |[_links](#) a|

|new_non_current_versions |integer a|Number of latest non-current versions to be retained.

|non_current_days |integer a|Number of days after which non-current versions can be deleted.

[#object_filter] [.api-collapsible-fifth-title] object_filter

Specifies a way to filter objects within a bucket.

[cols=3*,options=header]

|Name |Type |Description

|_links |[_links](#) a|

|prefix |string a|A prefix that is matched against object-names within a bucket.

|size_greater_than |integer a|Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.

|size_less_than |integer a|Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.

|tags |array[string] a|An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

[#svm] [.api-collapsible-fifth-title] svm

Specifies the name of the SVM where this bucket exists.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links a	
--------	----------	--

name	string a	The name of the SVM. This field cannot be specified in a PATCH method.
------	----------	--

uuid	string a	The unique identifier of the SVM. This field cannot be specified in a PATCH method.
------	----------	---

[#rules] [.api-collapsible-fifth-title] rules

Information about the lifecycle management rule of a bucket.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links a	
--------	----------	--

abort_incomplete_multipart_upload	abort_incomplete_multipart_upload a	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
-----------------------------------	-------------------------------------	--

bucket_name	string a	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
-------------	----------	--

enabled	boolean a	Specifies whether or not the associated rule is enabled.
---------	-----------	--

expiration	expiration a	Specifies a way to perform expiration action on filtered objects within a bucket.
------------	--------------	---

name	string a	Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.
------	----------	---

non_current_version_expiration	non_current_version_expiration a	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
--------------------------------	----------------------------------	---

object_filter	object_filter a	Specifies a way to filter objects within a bucket.
---------------	-----------------	--

svm	svm a	Specifies the name of the SVM where this bucket exists.
-----	-------	---

uuid	string a	Specifies the unique identifier of the bucket.
------	----------	--

[#lifecycle_management] [.api-collapsible-fifth-title] lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

|rules |array[[rules](#)] a|Specifies an object store lifecycle management policy. This field cannot be set using the PATCH method.

[#s3_bucket_policy_condition] [.api-collapsible-fifth-title] s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

[cols=3*,options=header]

|Name |Type |Description

|delimiters |array[string] a|An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.

|max_keys |array[integer] a|An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.

|operator |string a|Condition operator that is applied to the specified condition key.

|prefixes |array[string] a|An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.

|source_ips |array[string] a|An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.

|usernames |array[string] a|An array of usernames that a current user in the context is evaluated against using the condition operators.

[#s3_bucket_policy_statement] [.api-collapsible-fifth-title] s3_bucket_policy_statement

Specifies information about a single access permission.

[cols=3*,options=header]

|Name |Type |Description

|actions |array[string] a|

|conditions |array[[s3_bucket_policy_condition](#)] a|Specifies bucket policy conditions.

|effect |string a|Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.

|principals |array[string] a|

|resources |array[string] a|

|sid |string a|Specifies the statement identifier used to differentiate between statements. The sid length can range from 1 to 256 characters and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

[#policy] [.api-collapsible-fifth-title] policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

statements	array[s3_bucket_policy_statement]	a Specifies bucket access policy statement.
------------	-----------------------------------	---

[#destination] [.api-collapsible-fifth-title] destination

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

is_cloud	boolean	a Specifies whether a bucket is protected within the Cloud.
----------	---------	---

is_external_cloud	boolean	a Specifies whether a bucket is protected on external Cloud providers.
-------------------	---------	--

is_ontap	boolean	a Specifies whether a bucket is protected within ONTAP.
----------	---------	---

- Default value: 1
- readOnly: 1
- Introduced in: 9.10
- x-nullable: true

[#protection_status] [.api-collapsible-fifth-title] protection_status

Specifies attributes of bucket protection.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

destination	destination	a
-------------	-------------	---

is_protected	boolean	a Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be set in a POST method.
--------------	---------	---

- Default value: 1
- readOnly: 1
- Introduced in: 9.10
- x-nullable: true

[#qos_policy] [.api-collapsible-fifth-title] qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links	a
------------------------	------------------------	---

<code> max_throughput</code>	<code> string a </code>	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either <code>max_throughput_mbps</code> or <code>max_throughput_iops</code> are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
------------------------------	-------------------------	---

<code> max_throughput_iops</code>	<code> integer a </code>	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when <code>max_throughput</code> is set during POST or PATCH.
-----------------------------------	--------------------------	---

<code> max_throughput_mbps</code>	<code> integer a </code>	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when <code>max_throughput</code> is set during POST or PATCH.
-----------------------------------	--------------------------	--

<code> min_throughput</code>	<code> string a </code>	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either <code>min_throughput_mbps</code> or <code>min_throughput_iops</code> are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
------------------------------	-------------------------	--

<code> min_throughput_iops</code>	<code> integer a </code>	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when <code>min_throughput</code> is set during POST or PATCH.
-----------------------------------	--------------------------	--

<code> min_throughput_mbps</code>	<code> integer a </code>	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when <code>min_throughput</code> is set during POST or PATCH.
-----------------------------------	--------------------------	--

<code> name</code>	<code> string a </code>	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
--------------------	-------------------------	---

<code> uuid</code>	<code> string a </code>	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.
--------------------	-------------------------	---

[#retention] [.api-collapsible-fifth-title] retention

Specifies the retention mode and default retention period configured on the bucket.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

default_period	string a	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.
----------------	----------	--

mode	string a	The lock mode of the bucket. compliance ‐ A SnapLock Compliance (SLC) bucket provides the highest level of WORM protection and an administrator cannot destroy a compliance bucket if it contains unexpired WORM objects. governance ‐ An administrator can delete a Governance bucket. no_lock ‐ Indicates the bucket does not support object locking.
------	----------	--

[#snapshot_policy] [.api-collapsible-fifth-title] snapshot_policy

Specifies the bucket snapshot policy.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

name	string a	Specifies the name of the snapshot policy.
------	----------	--

uuid	string a	Specifies the unique identifier of the snapshot policy.
------	----------	---

[#svm] [.api-collapsible-fifth-title] svm

SVM, applies only to SVM-scoped objects.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links a	
--------	----------	--

name	string a	The name of the SVM. This field cannot be specified in a PATCH method.
------	----------	--

uuid	string a	The unique identifier of the SVM. This field cannot be specified in a PATCH method.
------	----------	---

```
[#volume] [.api-collapsible-fifth-title] volume
```

Specifies the FlexGroup volume name and UUID where the bucket is hosted. This field cannot be set in a POST method.

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

<code>_links</code>	<code>links</code>	a
---------------------	--------------------	---

<code>name</code>	string a	The name of the volume. This field cannot be specified in a PATCH method.
-------------------	----------	---

<code>uuid</code>	string a	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move.
-------------------	----------	---

- example: 028baa66-41bd-11e9-81d5-00a0986138f7
- Introduced in: 9.6
- x-nullable: true

```
[#error_arguments] [.api-collapsible-fifth-title] error_arguments
```

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

<code>code</code>	string a	Argument code
-------------------	----------	---------------

<code>message</code>	string a	Message argument
----------------------	----------	------------------

```
[#returned_error] [.api-collapsible-fifth-title] returned_error
```

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

<code>arguments</code>	array[error_arguments] a	Message arguments
------------------------	--	-------------------

<code>code</code>	string a	Error code
-------------------	----------	------------

<code>message</code>	string a	Error message
----------------------	----------	---------------

<code>target</code>	string a	The target parameter that caused the error.
---------------------	----------	---

====

= Update an S3 bucket configuration for an SVM

PATCH /protocols/s3/services/{svm.uuid}/buckets/{uuid}

Introduced In: 9.7

Updates the S3 bucket configuration of an SVM.

== Important notes

* The following fields can be modified for a bucket:

* **comment** - Any information related to the bucket.

* **size** - Bucket size.

* **policy** - An access policy for resources (buckets and objects) that defines their permissions. New policies are created after existing policies are deleted. To retain any of the existing policy statements, you need to specify those statements again. Policy conditions can also be modified using this API.

* **qos_policy** - A QoS policy for buckets.

* **audit_event_selector** - Audit policy for buckets. None can be specified for both access and permission to remove audit event selector.

* **versioning_state** - Versioning state for buckets.

* **nas_path** - NAS path to which the NAS bucket corresponds to.

* **retention.default_period** - Specifies the duration of default-retention applicable for objects on the object store bucket.

* **cors** - Specifying CORS rules enables the bucket to service the cross-origin requests. New CORS rules are created after existing rules are deleted. To retain any of the existing rules, you need to specify those CORS rules again. To remove all the existing CORS rules, specify an empty CORS rules list.

* **snapshot_policy** - Snapshot policy for the bucket.

* **is_consistent_etag** - Return a consistent ETag for NAS buckets.

== Related ONTAP commands

* vserver object-store-server bucket modify * vserver object-store-server bucket policy statement modify * vserver object-store-server bucket policy-statement-condition modify * vserver object-store-server bucket cors-rule create * vserver object-store-server bucket cors-rule delete

== Learn more

* [DOC /protocols/s3/services/{svm.uuid}/buckets](#)

|Name |Type |In |Required |Description

|uuid |string |path |True a|The unique identifier of the bucket.

|return_timeout |integer |query |False a|The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.

- Default value: 0
- Max value: 120
- Min value: 0

|svm.uuid |string |path |True a|UUID of the SVM to which this object belongs.

== Request Body

[cols=3*,options=header]

|Name |Type |Description

|audit_event_selector |[audit_event_selector](#) a|Event selector allows you to specify access and permission types to audit.

|comment |string a|Can contain any additional information about the bucket being created or modified.

|cors |[cors](#) a|Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

|encryption |[encryption](#) a|

|is_consistent_etag |boolean a|Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.

|lifecycle_management |[lifecycle_management](#) a|Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

|logical_used_size |integer a|Specifies the bucket logical used size up to this point. This field cannot be set using the PATCH method.

|nas_path |string a|Specifies the NAS path to which the nas bucket corresponds to.

|policy |[policy](#) a|A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

|protection_status |[protection_status](#) a|Specifies attributes of bucket protection.

|qos_policy |[qos_policy](#) a|Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

|retention |[retention](#) a|Specifies the retention mode and default retention period configured on the bucket.

|role |string a|Specifies the role of the bucket. This field cannot be set in a POST method.

|size |integer a|Specifies the bucket size in bytes; ranges from 190MB to 62PB.

|snapshot_policy |[snapshot_policy](#) a|Specifies the bucket snapshot policy.

|svm |[svm](#) a|SVM, applies only to SVM-scoped objects.

|type |string a|Specifies the bucket type. Valid values are "s3" and "nas". This field cannot be set using the PATCH method.

|uuid |string a|Specifies the unique identifier of the bucket. This field cannot be specified in a POST or PATCH method.

|versioning_state |string a|Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.

|volume |[volume](#) a|Specifies the FlexGroup volume name and UUID where the bucket is hosted. This field cannot be set in a POST method.


```
.Example request [%collapsible%closed] ===== [source,json,subs==+macros] { "audit_event_selector": {
"access": "string", "permission": "string", "comment": "S3 bucket.", "cors": { "rules": [ { "allowed_headers": [
"x-amz-request-id" ], "allowed_methods": [ "PUT", "DELETE" ], "allowed_origins": [ "http://www.example.com"
], "expose_headers": [ "x-amz-date" ], "id": "string", "max_age_seconds": 1024 } ] }, "is_nas_path_mutable":
true, "lifecycle_management": { "rules": [ { "expiration": { "object_age_days": 100, "object_expiry_date": "2039-
09-22 20:00:00 -0400" }, "svm": { "name": "svm1", "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7" },
"uuid": "414b29a1-3b26-11e9-bd58-0050568ea055" } ] }, "logical_used_size": 0, "nas_path": "/", "policy": {
"statements": [ { "actions": [ "GetObject", "PutObject", "DeleteObject", "ListBucket" ], "conditions": [ {
"delimiters": [ "/" ], "max_keys": [ 1000 ], "operator": "ip_address", "prefixes": [ "pref" ], "source_ips": [ "1.1.1.1",
"1.2.2.0/24" ], "usernames": [ "user1" ] } ], "effect": "allow", "principals": [ "user1", "group/grp1",
"nasgroup/group1" ], "resources": [ "bucket1", "bucket1/" ], "sid": "FullAccessToUser1" } ] }, "qos_policy":
{ "max_throughput": [ "900KB/s", "500MB/s", "120GB/s", "5000IOPS", "5000IOPS,500KB/s",
"2500IOPS,100MB/s", "1000IOPS,25MB/s" ], "max_throughput_iops": 10000,
"max_throughput_mbps": 500, "min_throughput": [ "900KB/s", "500MB/s", "120GB/s", "5000IOPS",
"5000IOPS,500KB/s", "2500IOPS,100MB/s", "1000IOPS,25MB/s" ], "min_throughput_iops": 2000,
"min_throughput_mbps": 500, "name": "performance", "uuid": "1cd8a442-86d1-11e0-ae1c-
123478563412" }, "retention": { "default_period": "P10Y" }, "role": "string", "size": 819200000,
"snapshot_policy": { "name": "default-1weekly", "uuid": "3675af31-431c-12fa-114a-20675afebc12" },
"svm": { "name": "svm1", "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7" }, "type": "s3", "uuid":
"string", "versioning_state": "enabled", "volume": { "name": "volume1", "uuid": "028baa66-41bd-
11e9-81d5-00a0986138f7" } } =====
```

== Response

```
` Status: 200, Ok `
```

[cols=3,options=header]

Name	Type	Description
------	------	-------------

job	job_link	a
-----	--------------------------	---

```
.Example response [%collapsible%closed] ===== [source,json,subs==+macros] { "job": { "uuid": "string" } } =====
```

== Response

```
` Status: 202, Accepted `
```

== Error

```
` Status: Default `
```

ONTAP Error Response Codes [cols=2*,options=header]

Error code	Message
------------	---------

92405778	"Failed to modify bucket "{bucket name}" for SVM "{svm.name}". Reason: {Reason for failure}."; 92405846
----------	--

92405811	"Failed to modify the object store volume. Reason: {Reason for failure}."; 92405811
----------	--

92405858	"Failed to modify bucket "{bucket name}" for SVM "{svm.name}". Wait a few minutes and try the operation again."; 92405858
----------	--

92405861	"Failed to "modify" the "bucket" because the operation is only supported on data SVMs."; 92405861
----------	--

92405863	"The specified "{parameter field}", "{parameter value}", does not exist."; 92405863
----------	--

92405864	"Failed to create access policies for bucket "{bucket name}". Reason: "Principal list can have a maximum of 10 entries.". Resolve all the issues and retry the operation."; 92405864
----------	---

|"An error occurs when deleting an access policy. The reason for failure is detailed in the error message."; |92405891
 |The resources specified in the access policy are not valid. Valid ways to specify a resource are *, <bucket-name>, <bucket-name>/.../.... Valid characters for a resource are 0-9, A-Z, a-z, _, +, comma, ;, :, =, ., &, @, ?, (,), single quote, *, !, - and \$.

|92405894

|"Statements, principals and resources list can have a maximum of 10 entries."; |92405897
 |The principals specified in the access policy are not in the correct format. User name must be in between 1 and 64 characters. Valid characters for a user name are 0-9, A-Z, a-z, _, +, =, comma, ., @, and - .

|92405898
|"The SID specified in the access policy is not valid. Valid characters for a SID are 0-9, A-Z and a-z."; |92405940
|"The specified condition key is not valid for operator "ip-address". Valid choices of keys for this operator: source-ips."; |92406014
|"Failed to modify event selector for bucket "{bucket name}". If value of either access or permission is set to none, then the other must be set to none as well."; |92406032
|"Modifying the NAS path for a NAS bucket is not supported."; |92406230
|"The value for "retention.default_period" parameter for object store bucket "<bucket>" cannot be greater than the maximum lock retention period set in the object store server for SVM "<SVM>". Check the maximum allowed lock retention period present in the object store server for SVM "<SVM>" and try the operation again."; //end row
 //start row |92406236 //end row //start row |"The value for "retention.default_period" parameter for object store bucket "<bucket>" cannot be less than the minimum lock retention period set in the object store server for SVM "<SVM>". Check the minimum allowed lock retention period present in the object store server for SVM "<SVM>" and try the operation again."; //end row //start row |92406217 //end row //start row |"The specified "allowed_headers" is not valid because it contains more than one wild card ("*") character."; //end row //start row |92406224 //end row //start row |"A Cross-Origin Resource Sharing (CORS) rule must have an origin and HTTP method specified."; //end row //start row |92406222 //end row //start row |"Cannot specify Cross-Origin Resource Sharing (CORS) configuration for object store bucket "<bucket>" on SVM "<SVM>". Specifying such configuration is supported on object store volumes created in ONTAP 9.8 or later releases only."; //end row
 //start row |92406211 //end row //start row |"The specified method "DONE" is not valid. Valid methods are GET, PUT, DELETE, HEAD, and POST."; //end row //start row |92405863 //end row //start row |"Failed to create CORS rules for bucket "bb1". Reason: "Field "index" cannot be specified for this operation.". Resolve all the issues and retry the operation."; //end row //start row |92406228 //end row //start row |"Cannot exceed the maximum limit of 100 Cross-Origin Resource Sharing (CORS) rules per S3 bucket "<bucket>" in SVM "<SVM>"."; //end row |=== //end
 table</SVM></bucket></SVM></bucket></SVM></SVM></bucket></SVM></SVM></bucket>

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

aggregates

Aggregate

Name	Type	Description
name	string	
uuid	string	

audit_event_selector

Event selector allows you to specify access and permission types to audit.

Name	Type	Description
access	string	Specifies read and write access types.
permission	string	Specifies allow and deny permission types.

rules

Information about the CORS rule of an S3 bucket.

Name	Type	Description
allowed_headers	array[string]	An array of HTTP headers allowed in the cross-origin requests.
allowed_methods	array[string]	An array of HTTP methods allowed in the cross-origin requests.
allowed_origins	array[string]	List of origins from where a cross-origin request is allowed to originate from for the S3 bucket.

Name	Type	Description
expose_headers	array[string]	List of extra headers sent in the response that customers can access from their applications.
id	string	Bucket CORS rule identifier. The length of the name can range from 0 to 256 characters.
max_age_seconds	integer	The time in seconds for your browser to cache the preflight response for the specified resource.

cors

Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.

Name	Type	Description
rules	array[rules]	Specifies an object store bucket CORS rule.

encryption

Name	Type	Description
enabled	boolean	Specifies whether encryption is enabled on the bucket. By default, encryption is disabled on a bucket. This field cannot be set in a POST or PATCH method.

abort_incomplete_multipart_upload

Specifies a way to perform `abort_incomplete_multipart_upload` action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
new_non_current_versions	integer	Number of latest non-current versions to be retained.
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
prefix	string	A prefix that is matched against object-names within a bucket.
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

rules

Information about the lifecycle management rule of a bucket.

Name	Type	Description
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

lifecycle_management

Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.

Name	Type	Description
rules	array[rules]	Specifies an object store lifecycle management policy. This field cannot be set using the PATCH method.

s3_bucket_policy_condition

Information about policy conditions based on various condition operators and condition keys.

Name	Type	Description
delimiters	array[string]	An array of delimiters that are compared with the delimiter value specified at the time of execution of an S3-based command, using the condition operator specified.
max_keys	array[integer]	An array of maximum keys that are allowed or denied to be retrieved using an S3 list operation, based on the condition operator specified.
operator	string	Condition operator that is applied to the specified condition key.
prefixes	array[string]	An array of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified.
source_ips	array[string]	An array of IP address ranges that are compared with the IP address of a source command at the time of execution of an S3-based command, using the condition operator specified.
usernames	array[string]	An array of usernames that a current user in the context is evaluated against using the condition operators.

s3_bucket_policy_statement

Specifies information about a single access permission.

Name	Type	Description
actions	array[string]	
conditions	array[s3_bucket_policy_condition]	Specifies bucket policy conditions.
effect	string	Specifies whether access is allowed or denied when a user requests the specific action. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
principals	array[string]	
resources	array[string]	
sid	string	Specifies the statement identifier used to differentiate between statements. The sid length can range from 1 to 256 characters and can only contain the following combination of characters 0-9, A-Z, and a-z. Special characters are not valid.

policy

A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.

Name	Type	Description
statements	array[s3_bucket_policy_statement]	Specifies bucket access policy statement.

destination

Name	Type	Description
is_cloud	boolean	Specifies whether a bucket is protected within the Cloud.

Name	Type	Description
is_external_cloud	boolean	Specifies whether a bucket is protected on external Cloud providers.
is_ontap	boolean	<p>Specifies whether a bucket is protected within ONTAP.</p> <ul style="list-style-type: none"> • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

protection_status

Specifies attributes of bucket protection.

Name	Type	Description
destination	destination	
is_protected	boolean	<p>Specifies whether a bucket is a source and if it is protected within ONTAP and/or an external cloud. This field cannot be set in a POST method.</p> <ul style="list-style-type: none"> • Default value: 1 • readOnly: 1 • Introduced in: 9.10 • x-nullable: true

qos_policy

Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

retention

Specifies the retention mode and default retention period configured on the bucket.

Name	Type	Description
default_period	string	Specifies the default retention period that is applied to objects while committing them to the WORM state without an associated retention period. The retention period can be in years, or days. The retention period value represents a duration and must be specified in the ISO-8601 duration format. A period specified for years and days is represented in the ISO-8601 format as "P<num>Y" and "P<num>D" respectively, for example "P10Y" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "P1Y10D" is not supported.</num></num>

snapshot_policy

Specifies the bucket snapshot policy.

Name	Type	Description
name	string	Specifies the name of the snapshot policy.
uuid	string	Specifies the unique identifier of the snapshot policy.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

volume

Specifies the FlexGroup volume name and UUID where the bucket is hosted. This field cannot be set in a POST method.

Name	Type	Description
name	string	The name of the volume. This field cannot be specified in a PATCH method.
uuid	string	Unique identifier for the volume. This corresponds to the instance-uuid that is exposed in the CLI and ONTAPI. It does not change due to a volume move. <ul style="list-style-type: none">• example: 028baa66-41bd-11e9-81d5-00a0986138f7• Introduced in: 9.6• x-nullable: true

s3_bucket_svm

A bucket is a container of objects. Each bucket defines an object namespace. S3 requests specify objects using a bucket-name and object-name pair. An object resides within a bucket.

Name	Type	Description
audit_event_selector	audit_event_selector	Event selector allows you to specify access and permission types to audit.
comment	string	Can contain any additional information about the bucket being created or modified.

Name	Type	Description
cors	cors	Cross-origin resource sharing (CORS) specifies an object associated with a bucket. The CORS configuration enables the bucket to service the cross-origin requests. A request might typically come from an origin with a domain that is different to that of the bucket. By configuring a CORS rule, you can define a combination of allowed origins, HTTP headers and methods that a bucket can use to filter out the cross-origin requests that it can service successfully.
encryption	encryption	
is_consistent_etag	boolean	Specifies whether the NAS bucket returns a consistent ETag across different S3 requests.
lifecycle_management	lifecycle_management	Lifecycle management is implemented as an object associated with a bucket. It defines rules to be applied against objects within a bucket. These rules are applied in the background and can delete objects.
logical_used_size	integer	Specifies the bucket logical used size up to this point. This field cannot be set using the PATCH method.
nas_path	string	Specifies the NAS path to which the nas bucket corresponds to.

Name	Type	Description
policy	policy	A policy is an object associated with a bucket. It defines resource (bucket, folder, or object) permissions. These policies get evaluated when an S3 user makes a request by executing a specific command. The user must be part of the principal (user or group) specified in the policy. Permissions in the policies determine whether the request is allowed or denied.
protection_status	protection_status	Specifies attributes of bucket protection.
qos_policy	qos_policy	Specifies "qos_policy.max_throughput_iops" and/or "qos_policy.max_throughput_mbps" or "qos_policy.min_throughput_iops" and/or "qos_policy.min_throughput_mbps". Specifying "min_throughput_iops" or "min_throughput_mbps" is only supported on volumes hosted on a node that is flash optimized. A pre-created QoS policy can also be used by specifying "qos_policy.name" or "qos_policy.uuid" properties. Setting or assigning a QoS policy to a bucket is not supported if its containing volume or SVM already has a QoS policy attached.
retention	retention	Specifies the retention mode and default retention period configured on the bucket.
role	string	Specifies the role of the bucket. This field cannot be set in a POST method.
size	integer	Specifies the bucket size in bytes; ranges from 190MB to 62PB.

Name	Type	Description
snapshot_policy	snapshot_policy	Specifies the bucket snapshot policy.
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Specifies the bucket type. Valid values are "s3" and "nas". This field cannot be set using the PATCH method.
uuid	string	Specifies the unique identifier of the bucket. This field cannot be specified in a POST or PATCH method.
versioning_state	string	Specifies the versioning state of the bucket. Valid values are "disabled", "enabled" or "suspended". Note that the versioning state cannot be modified to 'disabled' from any other state.
volume	volume	Specifies the FlexGroup volume name and UUID where the bucket is hosted. This field cannot be set in a POST method.

job_link

Name	Type	Description
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage S3 bucket lifecycle management rules

Manage S3 bucket lifecycle management rules

Overview

An S3 bucket lifecycle management rule is a list of objects. Each rule defines a set of actions to be performed on the object within the bucket.

Adding a lifecycle management rule on a S3 bucket under an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{uuid}/rules

# The call:
curl -iku admin:<password> -X POST "https://<mgmt-
ip>/api/protocols/s3/services/259b4e78-2893-67ea-9785-
890456bbbec4/buckets/259b4e46-2893-67ea-9145-
909456bbbec4/rules?return_timeout=0&return_records=true" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"name\":
\"rule1\", \"expiration\" : { \"object_age_days\" : \"1000\" },
\"abort_incomplete_multipart_upload\" : { \"after_initiation_days\" : 200
} , \"object_filter\": { \"prefix\" : \"obj1*/\" , \"size_greater_than\"
: \"1000\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 30 November 2022 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/259b4e78-2893-67ea-9785-
890456bbbec4/buckets/259b4e46-2893-67ea-9145-
909456bbbec4/rules?name=bucket-4
Content-Length: 353
Content-Type: application/json
{
  "job": {
    "uuid": "2e880171-7e16-11e9-bfdc-0050568ea123",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea123"
      }
    }
  }
}
```

Updating a lifecycle management rule on a S3 bucket under an SVM

```
# The call:
curl -iku admin:<password> -X PATCH "https://<mgmt-
ip>/api/protocols/s3/services/259b4e78-2893-67ea-9785-
890456bbbec4/buckets/259b4e46-2893-67ea-9145-
909456bbbec4/rules/rule1?return_timeout=0&return_records=true" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"expiration\"
: { \"object_age_days\" : \"3000\" },
\"abort_incomplete_multipart_upload\" : { \"after_initiation_days\" :
\"5000\" } }"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 30 November 2022 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/259b4e78-2893-67ea-9785-
890456bbbec4/buckets/259b4e46-2893-67ea-9145-
909456bbbec4/rules?name=bucket-4
Content-Length: 353
Content-Type: application/json
{
  "job": {
    "uuid": "2e880171-7e16-11e9-bfdc-0050568ea124",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea124"
      }
    }
  }
}
```

Deleting a lifecycle management rule on a S3 bucket under an SVM

```
# The call:
curl -X DELETE "https://<mgmt-ip>/api/protocols/s3/services/259b4e78-2893-
67ea-9785-890456bbbec4/buckets/259b4e46-2893-67ea-9145-
909456bbbec4/rules/rule1" -H "accept: application/json"
```

To delete an action within a rule, pass null inside the action-object.

```
# The call:
curl -iku admin:<password> -X PATCH "https://<mgmt-
ip>/api/protocols/s3/services/259b4e78-2893-67ea-9785-
890456bbbec4/buckets/259b4e46-2893-67ea-9145-
909456bbbec4/rules/rule1?return_timeout=0&return_records=true" -H "accept:
application/json" -H "Content-Type: application/json" -d '{"expiration\
: null }'"

# The response:
HTTP/1.1 202 Accepted
Date: Fri, 30 November 2022 11:22:14 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/259b4e78-2893-67ea-9785-
890456bbbec4/buckets/259b4e46-2893-67ea-9145-
909456bbbec4/rules?name=bucket-4
Content-Length: 353
Content-Type: application/json
{
  "job": {
    "uuid": "2e880171-7e16-11e9-bfdc-0050568ea124",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/2e880171-7e16-11e9-bfdc-0050568ea124"
      }
    }
  }
}
```

Retrieve S3 lifecycle rules for a bucket

GET /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/rules

Introduced In: 9.13

Retrieves all S3 Lifecycle rules associated with a bucket. Note that in order to retrieve S3 bucket rule parameters, the 'fields' option should be set to '**'.

Related ONTAP commands

- `vserver object-store-server bucket lifecycle-management-rule show`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/rules](#)

Parameters

Name	Type	In	Required	Description
uuid	string	query	False	Filter by uuid <ul style="list-style-type: none"> Introduced in: 9.14
name	string	query	False	Filter by name <ul style="list-style-type: none"> maxLength: 256 minLength: 0
bucket_name	string	query	False	Filter by bucket_name <ul style="list-style-type: none"> Introduced in: 9.14 maxLength: 63 minLength: 3
non_current_version_expiration.new_non_current_versions	integer	query	False	Filter by non_current_version_expiration.new_non_current_versions
non_current_version_expiration.non_current_days	integer	query	False	Filter by non_current_version_expiration.non_current_days
expiration.object_age_days	integer	query	False	Filter by expiration.object_age_days
expiration.expired_object_delete_marker	boolean	query	False	Filter by expiration.expired_object_delete_marker
expiration.object_expiry_date	string	query	False	Filter by expiration.object_expiry_date
object_filter.tags	string	query	False	Filter by object_filter.tags
object_filter.prefix	string	query	False	Filter by object_filter.prefix

Name	Type	In	Required	Description
object_filter.size_greater_than	integer	query	False	Filter by object_filter.size_greater_than
object_filter.size_less_than	integer	query	False	Filter by object_filter.size_less_than
enabled	boolean	query	False	Filter by enabled
abort_incomplete_multipart_upload.after_initiation_days	integer	query	False	Filter by abort_incomplete_multipart_upload.after_initiation_days
svm.name	string	query	False	Filter by svm.name <ul style="list-style-type: none"> Introduced in: 9.14
s3_bucket.uuid	string	path	True	The unique identifier of the bucket.
svm.uuid	string	path	True	UUID of the SVM to which this object belongs. <ul style="list-style-type: none"> Introduced in: 9.14
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. <ul style="list-style-type: none"> Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.</p> <ul style="list-style-type: none"> • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

Status: 200, Ok

Name	Type	Description
_links	collection_links	
num_records	integer	Number of records
records	array[s3_bucket_lifecycle_rule]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "abort_incomplete_multipart_upload": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        }
      },
      "bucket_name": "bucket1",
      "expiration": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        }
      },
      "object_age_days": 100,
      "object_expiry_date": "2039-09-22 20:00:00 -0400"
    },
    {
      "name": "string",
      "non_current_version_expiration": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        }
      },
      "object_filter": {
        "_links": {
```



```

        "self": {
            "href": "/api/resourcelink"
        },
        "prefix": "/logs",
        "size_greater_than": 10240,
        "size_less_than": 10485760,
        "tags": [
            "project1=projA",
            "project2=projB"
        ],
    },
    "svm": {
        "_links": {
            "self": {
                "href": "/api/resourcelink"
            }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055"
}
]
}

```

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

collection_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
_links	_links	
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
_links	_links	
new_non_current_versions	integer	Number of latest non-current versions to be retained.
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
_links	_links	
prefix	string	A prefix that is matched against object-names within a bucket.
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.

Name	Type	Description
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

s3_bucket_lifecycle_rule

Information about the lifecycle management rule of a bucket.

Name	Type	Description
_links	_links	
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
bucket_name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
name	string	Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
object_filter	object_filter	Specifies a way to filter objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.

Name	Type	Description
uuid	string	Specifies the unique identifier of the bucket.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create the S3 bucket lifecycle rule configuration

POST /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/rules

Introduced In: 9.13

Creates the S3 bucket lifecycle rule configuration.

Required properties

- `name` - Lifecycle Management rule to be created.
- `actions` - Lifecycle Management actions associated with the rule.

Recommended optional properties

- `enabled` - Lifecycle Management rule is enabled or not.
- `object_filter.prefix` - Lifecycle Management rule filter prefix.
- `object_filter.tags` - Lifecycle Management rule filter tags.
- `object_filter.size_greater_than` - Lifecycle Management rule filter minimum object size.

- `object_filter.size_less_than` - Lifecycle Management rule filter maximum object size.
- `object_age_days` - Number of days since creation after which objects can be deleted.
- `object_expiry_date` - Specific date from when objects can expire.
- `expired_object_delete_marker` - Cleanup object delete markers.
- `new_non_current_versions` - Number of latest non-current versions to be retained.
- `non_current_days` - Number of days after which non-current versions can be deleted.
- `after_initiation_days` - Number of days of initiation after which uploads can be aborted.

Related ONTAP commands

- `vserver object-store-server bucket lifecycle-management-rule create`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/rules](#)

Parameters

Name	Type	In	Required	Description
<code>s3_bucket.uuid</code>	string	path	True	Unique identifier of a bucket.

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none"> • Default value: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	<p>The default is false. If set to true, the records are returned.</p> <ul style="list-style-type: none"> • Default value:
svm.uuid	string	path	True	<p>UUID of the SVM to which this object belongs.</p> <ul style="list-style-type: none"> • Introduced in: 9.14

Request Body

Name	Type	Description
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
bucket_name	string	Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
enabled	boolean	Specifies whether or not the associated rule is enabled.
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
name	string	Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
object_filter	object_filter	Specifies a way to filter objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

Example request

```
{
  "bucket_name": "bucket1",
  "expiration": {
    "object_age_days": 100,
    "object_expiry_date": "2039-09-22 20:00:00 -0400"
  },
  "name": "string",
  "object_filter": {
    "prefix": "/logs",
    "size_greater_than": 10240,
    "size_less_than": 10485760,
    "tags": [
      "project1=projA",
      "project2=projB"
    ]
  },
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055"
}
```

Response

Status: 202, Accepted

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "uuid": "string"
  }
}
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Response

Status: 201, Created

Error

Status: Default

ONTAP Error Response Codes

Error code	Message
92405861	"The specified SVM UUID or bucket UUID does not exist.";
92406111	"Lifecycle Management rule "rule1" for bucket "testbuck1" in SVM "vs0" is invalid because of the number of tags specified. The maximum number of tags supported is four.";
92406113	"Lifecycle Management rule for bucket in Vserver is invalid because there is a mismatch in one of the filter-field. Filters must be the same for a particular rule identifier.";
92406114	"The Expiration action requires specifying either object_expiry_date, object_age_days or expired_object_delete_marker.";
92406115	"The NonCurrentVersionExpiration action requires either new_non_current_versions or non_current_days.";
92406116	"The AbortIncompleteMultipartUpload action requires after_initiation_days.";
92406117	"The "Expiration" action cannot have both an expiry date and an age.";
92406118	"Using Lifecycle Management rules requires an effective cluster version of 9.13.1 .";
92406120	"The "AbortIncompleteMultipartUpload" action cannot be specified with tags.";
92406121	""expired_object_delete_marker" cannot be specified with "tags"."

Error code	Message
92406122	""expired_object_delete_marker" cannot be specified with "object_age_days" or "object_expiry_date".";
92406123	"Expiration is supported on object store volumes only, bucket "testbuck-nas" on SVM "vs0" is not an object store volume.";
92406126	"Lifecycle Management rule "rule1" for bucket "testbuck1" in SVM "vs0" is invalid because specified tags contain one or more invalid characters. Valid characters for a tag are 0-9, A-Z, a-z, "+", "-", "=", ".", "_", ":", "/", "@", and " ". Each "=" character present in a tag key or value must be prefixed with the "" escape character.";
92406127	"Lifecycle Management rule "<rule>" for bucket "<bucket>" in SVM "<SVM>" is invalid because specified tag "key" length is greater than the maximum allowed length: 128."; //end row //start row
92406128 //end row //start row	"Lifecycle Management rule "rule1" for bucket "testbuck1" in SVM "vs0" has tags with duplicate keys. Verify that each tag has a unique key and then try the operation again."; //end row //start row
92406129 //end row //start row	"Lifecycle Management rule "rule1" for bucket "testbuck1" in SVM "vs0" has a prefix that is too long. The maximum length of the prefix is 1024 characters."; //end row //start row
92406130 //end row //start row	"Lifecycle Management rule "rule1" for bucket "testbuck1" in SVM "vs0" is invalid because the minimum object size of 10485760 is larger than or equal to the maximum object size of 10240."; //end row //start row
92406131 //end row //start row	"Lifecycle Management rule "testcheck2" for bucket "testbuck1" in SVM "vs0" cannot be created because "non_current_days" must be specified along with "new_non_current_versions"."; //end row //start row
92406132 //end row //start row	"Lifecycle Management rule "<rule>" for bucket "<bucket>" in SVM "<SVM>" requires "object_age_days" to be greater than zero."; //end row //start row
92406132 //end row //start row	"Lifecycle Management rule "<rule>" for bucket "<bucket>" in SVM "<SVM>" requires "new_non_current_versions" to be greater than zero."; //end row //start row
92406132 //end row //start row	"Lifecycle Management rule "<rule>" for bucket "<bucket>" in SVM "<SVM>" requires "after_initiation_days" to be greater than zero."; //end row //start row

Error code	Message
92406133 //end row //start row	"Lifecycle Management rule for bucket in Vserver is invalid. The object_expiry_date must be later than January 1, 1970."; //end row //start row
92406134 //end row //start row	"Cannot exceed the max limit of 1000 Lifecycle Management rules per bucket."; //end row //start row
92406135 //end row //start row	"MetroCluster is configured on cluster. Object Expiration is not supported in a MetroCluster configuration."; //end row //start row
92406136 //end row //start row	"Lifecycle Management rule "rule1" for bucket "buck1" in SVM "vs0" is invalid. The "object_expiry_date" must be at midnight GMT."; //end row //start row
92406139 //end row //start row	"Lifecycle Management rule for bucket in Vserver with action is a stale entry. Contact technical support for assistance."; //end row //start row
92406141 //end row //start row	"Lifecycle Management rule "rule1" for bucket "buck1" in SVM "vs0" with action "Expiration" cannot have "expired_object_delete_marker" disabled. To disable "expired_object_delete_marker", run the "vserver object-store-server bucket lifecycle-management-rule delete" command."; //end row //start row
92406143 //end row //start row	"As part of Bucket Lifecycle, cannot create fabriclink relationship on bucket "<bucket name="">" in SVM "<SVM name="">". Reason : <error>."; //end row //start row
92406144 //end row //start row	"The "AbortIncompleteMultipartUpload" action cannot be specified with object size."; //end row //start row
92406150 //end row //start row	""expired_object_delete_marker" cannot be specified with "size_less_than"."; //end row //start row
92406148 //end row //start row	"Lifecycle Management rule "rule1" for bucket "buck1" in SVM "vs0" cannot have "new_non_current_versions" more than 100."; //end row //start row
92406149 //end row //start row	"Lifecycle Management rule "rule1" for bucket "buck1" in SVM "vs0" requires an action to be specified. Retry the operation after adding an action."; //end row

|Name |Type |Description

|href |string a|

[#_links] [.api-collapsible-fifth-title] _links [#abort_incomplete_multipart_upload] [.api-collapsible-fifth-title] abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

[cols=3*,options=header]

|Name |Type |Description

|after_initiation_days |integer a|Number of days of initiation after which uploads can be aborted.

[#expiration] [.api-collapsible-fifth-title] expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

[cols=3*,options=header]

|Name |Type |Description

|expired_object_delete_marker |boolean a|Cleanup object delete markers.

|object_age_days |integer a|Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.

|object_expiry_date |string a|Specific date from when objects can expire. This cannot be used with object_age_days.

[#non_current_version_expiration] [.api-collapsible-fifth-title] non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

[cols=3*,options=header]

|Name |Type |Description

|new_non_current_versions |integer a|Number of latest non-current versions to be retained.

|non_current_days |integer a|Number of days after which non-current versions can be deleted.

[#object_filter] [.api-collapsible-fifth-title] object_filter

Specifies a way to filter objects within a bucket.

[cols=3*,options=header]

|Name |Type |Description

|prefix |string a|A prefix that is matched against object-names within a bucket.

|size_greater_than |integer a|Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.

|size_less_than |integer a|Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.

|tags |array[string] a|An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

```
[#svm] [.api-collapsible-fifth-title] svm
```

Specifies the name of the SVM where this bucket exists.

```
[cols=3*,options=header]
```

|Name |Type |Description

|name |string a|The name of the SVM. This field cannot be specified in a PATCH method.

|uuid |string a|The unique identifier of the SVM. This field cannot be specified in a PATCH method.

```
[#s3_bucket_lifecycle_rule] [.api-collapsible-fifth-title] s3_bucket_lifecycle_rule
```

Information about the lifecycle management rule of a bucket.

```
[cols=3*,options=header]
```

|Name |Type |Description

|abort_incomplete_multipart_upload |[abort_incomplete_multipart_upload](#) a|Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

|bucket_name |string a|Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".

|enabled |boolean a|Specifies whether or not the associated rule is enabled.

|expiration |[expiration](#) a|Specifies a way to perform expiration action on filtered objects within a bucket.

|name |string a|Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.

|non_current_version_expiration |[non_current_version_expiration](#) a|Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

|object_filter |[object_filter](#) a|Specifies a way to filter objects within a bucket.

|svm |[svm](#) a|Specifies the name of the SVM where this bucket exists.

|uuid |string a|Specifies the unique identifier of the bucket.

```
[#job_link] [.api-collapsible-fifth-title] job_link
```

```
[cols=3*,options=header]
```

|Name |Type |Description

|uuid |string a|The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

[#error_arguments] [.api-collapsible-fifth-title] error_arguments

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

code	string a	Argument code
------	----------	---------------

message	string a	Message argument
---------	----------	------------------

[#returned_error] [.api-collapsible-fifth-title] returned_error

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

arguments	array[error_arguments] a	Message arguments
-----------	--	-------------------

code	string a	Error code
------	----------	------------

message	string a	Error message
---------	----------	---------------

target	string a	The target parameter that caused the error.
--------	----------	---

====

= Delete an S3 bucket lifecycle rule

DELETE /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/rules/{name}

Introduced In: 9.13

Deletes the S3 bucket lifecycle rule configuration.

== Related ONTAP commands

* vserver object-store-server bucket lifecycle-management-rule delete

== Learn more

* [DOC /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/rules](#)

== Parameters

[cols=5*,options=header]

Name	Type	In	Required	Description
------	------	----	----------	-------------

s3_bucket.uuid	string path	True	a	The unique identifier of the bucket.
----------------	--------------	------	---	--------------------------------------

name	string path	True	a	The unique identifier of the bucket lifecycle_management rule.
------	--------------	------	---	--

svm.uuid	string path	True	a	UUID of the SVM to which this object belongs.
----------	--------------	------	---	---

- Introduced in: 9.14

== Response

` Status: 200, Ok `

== Error

` Status: Default `

ONTAP Error Response Codes [cols=2*,options=header]

| Error code | Message |92405861

|"The specified SVM UUID or bucket UUID does not exist."; |92406139

|"Lifecycle Management rule for bucket in Vserver with action is a stale entry. Contact technical support for assistance.";

[cols=3*,options=header]

|Name |Type |Description

|error |[returned_error](#) a|

.Example error [%collapsible%closed] ==== [source,json,subs=+macros] { "error": { "arguments": [{ "code": "string", "message": "string" }], "code": "4", "message": "entry doesn't exist", "target": "uuid" } } ====

== Definitions

[.api-def-first-level] .See Definitions [%collapsible%closed] ==== [#error_arguments] [.api-collapsible-fifth-title] error_arguments

[cols=3*,options=header]

|Name |Type |Description

|code |string a|Argument code

|message |string a|Message argument

[#returned_error] [.api-collapsible-fifth-title] returned_error

[cols=3*,options=header]

|Name |Type |Description

|arguments |array[error_arguments](#) a|Message arguments

|code |string a|Error code

|message |string a|Error message

|target |string a|The target parameter that caused the error.

=====

= Retrieve all S3 lifecycle rules for a bucket

GET /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/rules/{name}

Introduced In: 9.13

Retrieves all S3 Lifecycle rules associated with a bucket. Note that in order to retrieve S3 bucket rule parameters, the 'fields' option should be set to '**'.

== Related ONTAP commands

* **vserver object-store-server bucket lifecycle-management-rule show**

== Learn more

* [DOC /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/rules](#)

== Parameters

[cols=5,options=header]

Name	Type	In	Required	Description
------	------	----	----------	-------------

s3_bucket.uuid	string	path	True	a The unique identifier of the bucket.
----------------	--------	------	------	--

name	string	path	True	a The name of the lifecycle management rule to be applied on the bucket.
------	--------	------	------	--

svm.uuid	string	path	True	a UUID of the SVM to which this object belongs.
----------	--------	------	------	---

- Introduced in: 9.14

fields	array[string]	query	False	a Specify the fields to return.
--------	---------------	-------	-------	---------------------------------

== Response

```
` Status: 200, Ok `
```

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

_links	_links	a
--------	------------------------	---

abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	a Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
-----------------------------------	---	--

bucket_name	string	a Specifies the name of the bucket. Bucket name is a string that can only contain the following combination of ASCII-range alphanumeric characters 0-9, a-z, ".", and "-".
-------------	--------	--

enabled	boolean	a Specifies whether or not the associated rule is enabled.
---------	---------	--

expiration	expiration	a Specifies a way to perform expiration action on filtered objects within a bucket.
------------	----------------------------	---

|name |string a|Bucket lifecycle management rule identifier. The length of the name can range from 0 to 256 characters.

|non_current_version_expiration |[non_current_version_expiration](#) a|Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

|object_filter |[object_filter](#) a|Specifies a way to filter objects within a bucket.

|svm |[svm](#) a|Specifies the name of the SVM where this bucket exists.

|uuid |string a|Specifies the unique identifier of the bucket.

```
.Example response [%collapsible%closed] ==== [source,json,subs=+macros] { "_links": { "self": { "href":  
"/api/resourcelink" } }, "abort_incomplete_multipart_upload": { "_links": { "self": { "href": "/api/resourcelink" } } },  
"bucket_name": "bucket1", "expiration": { "_links": { "self": { "href": "/api/resourcelink" } } }, "object_age_days":  
100, "object_expiry_date": "2039-09-22 20:00:00 -0400", "name": "string", "non_current_version_expiration":  
{ "_links": { "self": { "href": "/api/resourcelink" } } }, "object_filter": { "_links": { "self": { "href": "/api/resourcelink" }  
}, "prefix": "/logs", "size_greater_than": 10240, "size_less_than": 10485760, "tags": [ "project1=projA",  
"project2=projB" ] }, "svm": { "_links": { "self": { "href": "/api/resourcelink" } }, "name": "svm1", "uuid":  
"02c9e252-41be-11e9-81d5-00a0986138f7", "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055" } =====
```

== Error

```
` Status: Default, Error `
```

[cols=3*,options=header]

|Name |Type |Description

|error |[returned_error](#) a|

```
.Example error [%collapsible%closed] ==== [source,json,subs=+macros] { "error": { "arguments": [ { "code":  
"string", "message": "string" } ], "code": "4", "message": "entry doesn't exist", "target": "uuid" } } =====
```

== Definitions

[.api-def-first-level] .See Definitions [%collapsible%closed] ==== [#href] [.api-collapsible-fifth-title] href

[cols=3*,options=header]

|Name |Type |Description

|href |string a|

[#_links] [.api-collapsible-fifth-title] _links

[cols=3*,options=header]

|Name |Type |Description

|self |[href](#) a|

[#abort_incomplete_multipart_upload] [.api-collapsible-fifth-title] abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

[cols=3*,options=header]

|Name |Type |Description

|_links |[_links](#) a|

|after_initiation_days |integer a|Number of days of initiation after which uploads can be aborted.

[#expiration] [.api-collapsible-fifth-title] expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

[cols=3*,options=header]

|Name |Type |Description

|_links |[_links](#) a|

|expired_object_delete_marker |boolean a|Cleanup object delete markers.

|object_age_days |integer a|Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.

|object_expiry_date |string a|Specific date from when objects can expire. This cannot be used with object_age_days.

[#non_current_version_expiration] [.api-collapsible-fifth-title] non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

[cols=3*,options=header]

|Name |Type |Description

|_links |[_links](#) a|

|new_non_current_versions |integer a|Number of latest non-current versions to be retained.

|non_current_days |integer a|Number of days after which non-current versions can be deleted.

[#object_filter] [.api-collapsible-fifth-title] object_filter

Specifies a way to filter objects within a bucket.

[cols=3*,options=header]

|Name |Type |Description

|_links |[_links](#) a|

|prefix |string a|A prefix that is matched against object-names within a bucket.

|size_greater_than |integer a|Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.

|size_less_than |integer a|Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.

|tags |array[string] a|An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

```
[#svm] [.api-collapsible-fifth-title] svm
```

Specifies the name of the SVM where this bucket exists.

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

|_links |[_links](#) a|

|name |string a|The name of the SVM. This field cannot be specified in a PATCH method.

|uuid |string a|The unique identifier of the SVM. This field cannot be specified in a PATCH method.

```
[#error_arguments] [.api-collapsible-fifth-title] error_arguments
```

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

|code |string a|Argument code

|message |string a|Message argument

```
[#returned_error] [.api-collapsible-fifth-title] returned_error
```

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

|arguments |array[[error_arguments](#)] a|Message arguments

|code |string a|Error code

|message |string a|Error message

|target |string a|The target parameter that caused the error.

=====

= Update the S3 bucket lifecycle rule configuration

PATCH /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/rules/{name}

Introduced In: 9.13

Updates the S3 bucket lifecycle rule configuration.

== Important notes

* The following fields can be modified for a bucket: * `actions` - Lifecycle Management actions associated with the rule. * `enabled` - Lifecycle Management rule is enabled or not.. * `object_age_days` - Number of days since creation after which objects can be deleted. * `object_expiry_date` - Specific date from when objects can expire. * `expired_object_delete_marker` - Cleanup object delete markers. * `new_non_current_versions` - Number of latest non-current versions to be retained. * `non_current_days` - Number of days after which non-current versions can be deleted. * `after_initiation_days` - Number of days of initiation after which uploads can be aborted.

== Related ONTAP commands

* `vserver object-store-server bucket lifecycle-management-rule modify`

== Learn more

* [DOC /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/rules](#)

== Parameters

[cols=5*,options=header]

Name	Type	In	Required	Description
------	------	----	----------	-------------

s3_bucket.uuid	string	path	True	a The unique identifier of the bucket.
----------------	--------	------	------	--

name	string	path	True	a The name of the lifecycle management rule to be applied on the bucket.
------	--------	------	------	--

return_timeout	integer	query	False	a The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.
----------------	---------	-------	-------	--

- Default value: 0
- Max value: 120
- Min value: 0

svm.uuid	string	path	True	a UUID of the SVM to which this object belongs.
----------	--------	------	------	---

- Introduced in: 9.14

== Request Body

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	a Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
-----------------------------------	---	--

enabled	boolean	a Specifies whether or not the associated rule is enabled.
---------	-------------------------	--

expiration	expiration	a Specifies a way to perform expiration action on filtered objects within a bucket.
------------	----------------------------	---

non_current_version_expiration	non_current_version_expiration	a Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
--------------------------------	--	---

svm	svm	a Specifies the name of the SVM where this bucket exists.
-----	---------------------	---

uuid	string	a Specifies the unique identifier of the bucket.
------	------------------------	--

```
.Example request [%collapsible%closed] ==== [source,json,subs=+macros] { "expiration": {  
"object_age_days": 100, "object_expiry_date": "2039-09-22 20:00:00 -0400" }, "svm": { "name": "svm1",  
"uuid": "02c9e252-41be-11e9-81d5-00a0986138f7" }, "uuid": "414b29a1-3b26-11e9-bd58-0050568ea055" }  
====
```

== Response

```
` Status: 200, Ok `
```

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

num_records	integer	a Number of records
-------------	-------------------------	---------------------

records	array[s3_bucket_lifecycle_rule]	a
---------	---	---

```
.Example response [%collapsible%closed] ==== [source,json,subs=+macros] { "num_records": 1, "records": [  
{ "expiration": { "object_age_days": 100, "object_expiry_date": "2039-09-22 20:00:00 -0400" }, "svm": {  
"name": "svm1", "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7" }, "uuid": "414b29a1-3b26-11e9-bd58-  
0050568ea055" } ] }  
====
```

== Response

```
` Status: 202, Accepted `
```

== Error

```
` Status: Default `
```

ONTAP Error Response Codes [cols=2*,options=header]

Error code	Message	92405861 "The specified SVM UUID or bucket UUID does not exist.";
------------	---------	---

|92406114
|"The Expiration action requires specifying either object_expiry_date, object_age_days or expired_object_delete_marker."; |92406115
|"The NonCurrentVersionExpiration action requires either new_non_current_versions or non_current_days."; |92406116
|"The AbortIncompleteMultipartUpload action requires after_initiation_days."; |92406117
|"The "Expiration" action cannot have both an expiry date and an age."; |92406118
|"Using Lifecycle Management rules requires an effective cluster version of 9.13.1 ."; |92406122
|"expired_object_delete_marker" cannot be specified with "object_age_days" or "object_expiry_date"."; |92406131
|"Lifecycle Management rule "testcheck2" for bucket "testbuck1" in SVM "vs0" cannot be created because "non_current_days" must be specified along with "new_non_current_versions"."; |92406132
|"Lifecycle Management rule "<rule>" for bucket "<bucket>" in SVM "<SVM>" requires "object_age_days" to be greater than zero."; //end row //start row |92406132 //end row //start row |"Lifecycle Management rule "<rule>" for bucket "<bucket>" in SVM "<SVM>" requires "new_non_current_versions" to be greater than zero."; //end row //start row |92406132 //end row //start row |"Lifecycle Management rule "<rule>" for bucket "<bucket>" in SVM "<SVM>" requires "after_initiation_days" to be greater than zero."; //end row //start row |92406133 //end row //start row |"Lifecycle Management rule for bucket in Vserver is invalid. The object_expiry_date must be later than January 1, 1970."; //end row //start row |92406135 //end row //start row |"MetroCluster is configured on cluster. Object Expiration is not supported in a MetroCluster configuration."; //end row //start row |92406136 //end row //start row |"Lifecycle Management rule "rule1" for bucket "buck1" in SVM "vs0" is invalid. The "object_expiry_date" must be at midnight GMT."; //end row //start row |92406139 //end row //start row |"Lifecycle Management rule for bucket in Vserver with action is a stale entry. Contact technical support for assistance."; //end row //start row |92406142 //end row //start row |"Lifecycle Management rule "rule1" for bucket "buck1" in SVM "vs0" with action "Expiration" cannot have "expired_object_delete_marker" disabled. To disable "expired_object_delete_marker", run the "vserver object-store-server bucket lifecycle-management-rule delete" command."; //end row //start row |92406146 //end row //start row |"Lifecycle Management rule "rule1" for bucket "buck1" in SVM "vs0" already exists. Delete the rule and then try the operation again."; //end row //start row |92406148 //end row //start row |"Lifecycle Management rule "rule1" for bucket "buck1" in SVM "vs0" cannot have "new_non_current_versions" more than 100."; //end row //start row |92406149 //end row //start row |"Lifecycle Management rule "rule1" for bucket "buck1" in SVM "vs0" requires an action to be specified. Retry the operation after adding an action."; //end row |=== //end table</SVM></bucket></rule></SVM></bucket></rule></SVM></bucket></rule>

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

abort_incomplete_multipart_upload

Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.

Name	Type	Description
after_initiation_days	integer	Number of days of initiation after which uploads can be aborted.

expiration

Specifies a way to perform expiration action on filtered objects within a bucket.

Name	Type	Description
expired_object_delete_marker	boolean	Cleanup object delete markers.
object_age_days	integer	Number of days since creation after which objects can be deleted. This cannot be used along with object_expiry_date.
object_expiry_date	string	Specific date from when objects can expire. This cannot be used with object_age_days.

non_current_version_expiration

Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.

Name	Type	Description
new_non_current_versions	integer	Number of latest non-current versions to be retained.
non_current_days	integer	Number of days after which non-current versions can be deleted.

object_filter

Specifies a way to filter objects within a bucket.

Name	Type	Description
prefix	string	A prefix that is matched against object-names within a bucket.
size_greater_than	integer	Size of the object greater than specified for which the corresponding lifecycle rule is to be applied.
size_less_than	integer	Size of the object smaller than specified for which the corresponding lifecycle rule is to be applied.
tags	array[string]	An array of key-value paired tags of the form <tag>or <tag=value>.</tag>

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

s3_bucket_lifecycle_rule

Information about the lifecycle management rule of a bucket.

Name	Type	Description
abort_incomplete_multipart_upload	abort_incomplete_multipart_upload	Specifies a way to perform abort_incomplete_multipart_upload action on filtered objects within a bucket. It cannot be specified with tags.
enabled	boolean	Specifies whether or not the associated rule is enabled.

Name	Type	Description
expiration	expiration	Specifies a way to perform expiration action on filtered objects within a bucket.
non_current_version_expiration	non_current_version_expiration	Specifies a way to perform non_current_version_expiration action on filtered objects within a bucket.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	Specifies the unique identifier of the bucket.

collection_links

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage S3 bucket snapshots

Manage S3 bucket snapshots

Overview

An S3 bucket snapshot is an image of the bucket as it exists at the time when the snapshot is created.

S3 bucket snapshots can be created using scheduled snapshot policies set on the bucket, or user requested snapshot creations.

S3 bucket snapshot APIs allow you to create, delete, and retrieve snapshots.

Snapshot APIs

The following APIs are used to perform operations related to snapshots.

– POST /api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots

– GET /api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots

– GET /api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots/{uuid}

– DELETE /api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots/{uuid}

Examples

Creating an S3 bucket snapshot

The POST operation is used to create an S3 bucket snapshot with the specified name.

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots:

# The call:
curl -X POST -k "https://<mgmt-
ip>/api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshot
s" -H "accept: application/json" -d '{"name" : "ss1"}'

# The response:
{
  "job": {
    "uuid": "af10a4d1-60b3-11ef-82cf-005056ae1130",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/af10a4d1-60b3-11ef-82cf-005056ae1130"
      }
    }
  }
}

# The Job:
{
  "uuid": "af10a4d1-60b3-11ef-82cf-005056ae1130",
  "description": "POST /api/protocols/s3/services/148b9bbd-58d8-11ef-b7ca-
005056ae1130/buckets/2aec8270-58e3-11ef-861e-
005056ae1130/snapshots/?name=ss1",
```

```
"state": "success",
"message": "success",
"code": 0,
"start_time": "2024-08-22T14:23:52-04:00",
"end_time": "2024-08-22T14:23:54-04:00",
"svm": {
  "name": "vs0",
  "uuid": "148b9bbd-58d8-11ef-b7ca-005056ae1130",
  "_links": {
    "self": {
      "href": "/api/svm/svms/148b9bbd-58d8-11ef-b7ca-005056ae1130"
    }
  }
},
"_links": {
  "self": {
    "href": "/api/cluster/jobs/af10a4d1-60b3-11ef-82cf-005056ae1130"
  }
}
}
```

Retrieving S3 bucket snapshots

The GET operation is used to retrieve all S3 bucket snapshots for a specific bucket.

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots:

# The call:
curl -X GET -k "https://<mgmt-
ip>/api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshot
s" -H "accept: application/json"

# The response:
{
  "records": [
    {
      "uuid": "20837456-3c8b-405a-aa3a-5300c048f87d",
      "name": "ss1"
    },
    {
      "uuid": "c67cd056-d386-477a-8378-fcc06987bedf",
      "name": "ss2"
    }
  ],
  "num_records": 2
}
```

Retrieving S3 bucket snapshots and all snapshot attributes

The GET operation is used to retrieve all S3 bucket snapshots for a specific bucket along with all the snapshot attributes.

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots:

# The call:
curl -X GET -k "https://<mgmt-
ip>/api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshot
s?fields=*" -H "accept: application/json"

# The response:
{
  "records": [
    {
      "svm": {
        "uuid": "148b9bbd-58d8-11ef-b7ca-005056ae1130"
      },
      "bucket": {
        "uuid": "2aec8270-58e3-11ef-861e-005056ae1130"
      },
      "uuid": "20837456-3c8b-405a-aa3a-5300c048f87d",
      "name": "ss1",
      "create_time": "2024-08-22T14:23:54-04:00"
    },
    {
      "svm": {
        "uuid": "148b9bbd-58d8-11ef-b7ca-005056ae1130"
      },
      "bucket": {
        "uuid": "2aec8270-58e3-11ef-861e-005056ae1130"
      },
      "uuid": "c67cd056-d386-477a-8378-fcc06987bedf",
      "name": "ss2",
      "create_time": "2024-08-22T14:30:42-04:00"
    }
  ],
  "num_records": 2
}
```

Retrieving the attributes of a specific S3 bucket snapshot

The GET operation is used to retrieve the attributes of a specific S3 bucket snapshot.

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots/{
uuid}:

# The call:
curl -X GET -k "https://<mgmt-
ip>/api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshot
s/{uuid}" -H "accept: application/json"

# The response:
{
  "svm": {
    "uuid": "148b9bbd-58d8-11ef-b7ca-005056ae1130"
  },
  "bucket": {
    "uuid": "2aec8270-58e3-11ef-861e-005056ae1130"
  },
  "uuid": "c67cd056-d386-477a-8378-fcc06987bedf",
  "name": "ss2",
  "create_time": "2024-08-22T14:30:42-04:00"
}
```

Deleting an S3 bucket snapshot

The DELETE operation is used to delete an S3 bucket snapshot.

```
# The API:
/api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots/{
uuid}:

# The call:
curl -X DELETE -k "https://<mgmt-
ip>/api/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshot
s/{uuid}" -H "accept: application/json"

# The response:
{
  "job": {
    "uuid": "94f97fa9-60b7-11ef-82cf-005056ae1130",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/94f97fa9-60b7-11ef-82cf-005056ae1130"
      }
    }
  }
}
```



```

}

# The Job:
{
  "uuid": "94f97fa9-60b7-11ef-82cf-005056ae1130",
  "description": "DELETE /api/protocols/s3/services/148b9bbd-58d8-11ef-b7ca-005056ae1130/buckets/2aec8270-58e3-11ef-861e-005056ae1130/snapshots/c67cd056-d386-477a-8378-fcc06987bedf",
  "state": "success",
  "message": "success",
  "code": 0,
  "start_time": "2024-08-22T14:51:46-04:00",
  "end_time": "2024-08-22T14:51:47-04:00",
  "svm": {
    "name": "vs0",
    "uuid": "148b9bbd-58d8-11ef-b7ca-005056ae1130",
    "_links": {
      "self": {
        "href": "/api/svm/svms/148b9bbd-58d8-11ef-b7ca-005056ae1130"
      }
    }
  },
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/94f97fa9-60b7-11ef-82cf-005056ae1130"
    }
  }
}

```

Retrieve a collection of S3 bucket snapshots

GET /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots

Introduced In: 9.16

Retrieves a collection of S3 bucket snapshots.

Related ONTAP commands

- `vserver object-store-server bucket snapshot show`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots](#)

Parameters

Name	Type	In	Required	Description
s3_bucket.uuid	string	path	True	The unique identifier of the bucket.
svm.name	string	query	False	Filter by svm.name
name	string	query	False	Filter by name
bucket_uuid	string	query	False	Filter by bucket_uuid
uuid	string	query	False	Filter by uuid
create_time	string	query	False	Filter by create_time
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	<p>The default is true for GET calls. When set to false, only the number of records is returned.</p> <ul style="list-style-type: none"> • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.</p> <ul style="list-style-type: none"> • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

Status: 200, Ok

Name	Type	Description
_links	collection_links	
num_records	integer	Number of records
records	array[s3_bucket_snapshot]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "bucket_uuid": "2aec8270-58e3-11ef-861e-005056ae1130",
      "create_time": "2024-08-21 20:18:04 -0400",
      "name": "snap1",
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "uuid": "522b29a1-3b26-11e9-bd58-0050568ea321"
    }
  ]
}
```

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

collection_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

s3_bucket_snapshot

Information about an S3 bucket snapshot.

Name	Type	Description
_links	_links	
bucket_uuid	string	The unique identifier of the bucket.
create_time	string	Creation time of the snapshot. It is the storage unit access time when the snapshot was created.

Name	Type	Description
name	string	The name of the snapshot. Snapshot names must start with a lowercase letter, a number, or a hyphen, must end with a lowercase letter or a number, and cannot exceed 30 characters.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	The UUID of the snapshot in the bucket that uniquely identifies the snapshot in that bucket.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create an S3 bucket snapshot

POST /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots

Introduced In: 9.16

Creates an S3 bucket snapshot.

Required properties

- `name` - Name of the S3 bucket snapshot to be created.

Related ONTAP commands

- `vserver object-store-server bucket snapshot create`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots](#)

Parameters

Name	Type	In	Required	Description
s3_bucket.uuid	string	path	True	Unique identifier of a bucket.
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202.</p> <ul style="list-style-type: none">• Default value: 0• Max value: 120• Min value: 0

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
bucket_uuid	string	The unique identifier of the bucket.
create_time	string	Creation time of the snapshot. It is the storage unit access time when the snapshot was created.
name	string	The name of the snapshot. Snapshot names must start with a lowercase letter, a number, or a hyphen, must end with a lowercase letter or a number, and cannot exceed 30 characters.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	The UUID of the snapshot in the bucket that uniquely identifies the snapshot in that bucket.

Example request

```
{
  "bucket_uuid": "2aec8270-58e3-11ef-861e-005056ae1130",
  "create_time": "2024-08-21 20:18:04 -0400",
  "name": "snap1",
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "522b29a1-3b26-11e9-bd58-0050568ea321"
}
```

Response

Status: 202, Accepted

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "uuid": "string"
  }
}
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Response

Status: 201, Created

Error

Status: Default

ONTAP Error Response Codes

Error code	Message
92405861	"The specified SVM UUID or bucket UUID does not exist.";
92406249	"Failed to create S3 bucket snapshot "{snapshot name}" for S3 bucket "{bucket name}" in SVM "{svm name}". Reason: {Reason for failure} ";

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

s3_bucket_snapshot

Information about an S3 bucket snapshot.

Name	Type	Description
bucket_uuid	string	The unique identifier of the bucket.
create_time	string	Creation time of the snapshot. It is the storage unit access time when the snapshot was created.
name	string	The name of the snapshot. Snapshot names must start with a lowercase letter, a number, or a hyphen, must end with a lowercase letter or a number, and cannot exceed 30 characters.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	The UUID of the snapshot in the bucket that uniquely identifies the snapshot in that bucket.

job_link

Name	Type	Description
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete an S3 bucket snapshot

DELETE

/protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots/{uuid}

Introduced In: 9.16

Deletes S3 bucket snapshot.

Related ONTAP commands

- `vserver object-store-server bucket snapshot delete`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots](#)

Parameters

Name	Type	In	Required	Description
s3_bucket.uuid	string	path	True	The unique identifier of the bucket.
uuid	string	path	True	The unique identifier of the S3 bucket snapshot.
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Response

Status: 200, Ok

Error

Status: Default

ONTAP Error Response Codes

Error code	Message
92405861	"The specified SVM UUID or bucket UUID does not exist.";
92406250	"Failed to delete S3 bucket snapshot "{snapshot name}" for S3 bucket "{bucket name}" in SVM "{svm name}". Reason: {Reason for failure} ";
92406278	"Failed to delete S3 bucket snapshot with UUID "{snapshot uuid}" for S3 bucket "{bucket name}" in SVM "{svm name}". Reason: {Reason for failure} ";

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve details of a specific S3 bucket snapshot

GET /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots/{uuid}

Introduced In: 9.16

Retrieves details of a specific S3 bucket snapshot.

Related ONTAP commands

- `vserver object-store-server bucket snapshot show`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/buckets/{s3_bucket.uuid}/snapshots](#)

Parameters

Name	Type	In	Required	Description
s3_bucket.uuid	string	path	True	The unique identifier of the bucket.
uuid	string	path	True	The unique identifier of the S3 bucket snapshot.
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.

Response

Status: 200, Ok

Name	Type	Description
_links	_links	
bucket_uuid	string	The unique identifier of the bucket.
create_time	string	Creation time of the snapshot. It is the storage unit access time when the snapshot was created.

Name	Type	Description
name	string	The name of the snapshot. Snapshot names must start with a lowercase letter, a number, or a hyphen, must end with a lowercase letter or a number, and cannot exceed 30 characters.
svm	svm	Specifies the name of the SVM where this bucket exists.
uuid	string	The UUID of the snapshot in the bucket that uniquely identifies the snapshot in that bucket.

Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "bucket_uuid": "2aec8270-58e3-11ef-861e-005056ae1130",
  "create_time": "2024-08-21 20:18:04 -0400",
  "name": "snap1",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "522b29a1-3b26-11e9-bd58-0050568ea321"
}
```

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

svm

Specifies the name of the SVM where this bucket exists.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage S3 service group configuration

Manage S3 service group configuration

Overview

An S3 group consists of one or many users. Policies are attached to the S3 group to have access control over S3 resources at group level.

Examples

Retrieving all fields for all S3 groups of an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/groups:

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-0050568ea123/groups?fields=*&return_records=true&return_timeout=15" -H "accept: application/json"

# The response:
{
  "records": [
    {
      "comment": "Admin group",
      "id": 5,
      "name": "Admin-Group",
      "policies": [
        { "name": "Policy1" },
        { "name": "Policy2" },
        { "name": "Policy3" }
      ],
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "users": [
        { "name": "User1" },
        { "name": "User2" },
        { "name": "User3" }
      ]
    },
    {
      "comment": "Admin group",
      "id": 6,
```

```
"name": "Admin-Group1",
"policies": [
  { "name": "Policy1" },
  { "name": "Policy2" },
  { "name": "Policy3" }
],
"svm": {
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"users": [
  { "name": "User1" },
  { "name": "User2" },
  { "name": "User6" }
]
}
],
"num_records": 2
}
```

Retrieving the specified group in the SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/groups/{group_id}:

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-0050568ea123/groups/5?fields=*" -H "accept: application/json"

# The response:
{
  "comment": "Admin group",
  "id": 5,
  "name": "Admin-Group",
  "policies": [
    { "name": "Policy1" },
    { "name": "Policy2" },
    { "name": "Policy3" }
  ],
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "users": [
    { "name": "User1" },
    { "name": "User2" },
    { "name": "User3" }
  ]
}
```

Creating an S3 group for an SVM

```

# The API:
/api/protocols/s3/services/{svm.uuid}/groups

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-0050568ea123/groups?return_records=true" -H "accept: application/json" -H "authorization: Basic <CREDENTIALS>" -H "Content-Type: application/json" -d "{ \"comment\": \"Admin group\", \"name\": \"Admin-Group\", \"policies\": [ { \"name\": \"Policy1\" }, { \"name\": \"Policy2\" }, { \"name\": \"Policy3\" } ], \"users\": [ { \"name\": \"User1\" }, { \"name\": \"User2\" }, { \"name\": \"User3\" } ] }"

# The response:
HTTP/1.1 202 Accepted
Date: Mon, 16 Mar 2020 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 289
Content-Type: application/json
{
  "num_records": 1,
  "records": [
    {
      "comment": "Admin group",
      "id": 5,
      "name": "Admin-Group",
      "policies": [
        { "name": "Policy1" },
        { "name": "Policy2" },
        { "name": "Policy3" }
      ],
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "users": [
        { "name": "User1" },
        { "name": "User2" },
        { "name": "User3" }
      ]
    }
  ]
}

```

Updating an S3 group for an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/groups/{group_id}:

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-0050568ea123/groups/5" -H "accept: application/json" -H
"authorization: Basic <CREDENTIALS>" -H "Content-Type: application/json"
-d "{ \"comment\": \"Admin group\", \"name\": \"Admin-Group\",
\"policies\": [ { \"name\": \"Policy1\" } ], \"users\": [ { \"name\":
\"user-1\" } ]}"

# The response:
HTTP/1.1 202 Accepted
Date: Mon, 16 Mar 2020 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
```

Deleting an S3 group for a specified SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/groups/{group_id}:

# The call:
curl -X DELETE "https://<mgmt-ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-0050568ea123/groups/5" -H "accept: application/json"

# The response:
HTTP/1.1 202 Accepted
Date: Mon, 16 Mar 2020 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
```

Retrieve an S3 group configuration

GET /protocols/s3/services/{svm.uuid}/groups

Introduced In: 9.8

Retrieves the S3 group's SVM configuration.

Related ONTAP commands

- `vserver object-store-server group show`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/groups](#)

Parameters

Name	Type	In	Required	Description
name	string	query	False	Filter by name <ul style="list-style-type: none">• maxLength: 128• minLength: 1
comment	string	query	False	Filter by comment <ul style="list-style-type: none">• maxLength: 256• minLength: 0
policies.name	string	query	False	Filter by policies.name <ul style="list-style-type: none">• maxLength: 128• minLength: 1
id	integer	query	False	Filter by id
users.name	string	query	False	Filter by users.name <ul style="list-style-type: none">• maxLength: 64• minLength: 1
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

Status: 200, Ok

Name	Type	Description
_links	collection_links	
num_records	integer	Number of records
records	array[s3_group]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "comment": "Admin group",
      "id": 5,
      "name": "Admin-Group",
      "policies": [
        {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "Policy1"
        }
      ],
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "users": [
        {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "user-1"
        }
      ]
    }
  ]
}
```

```
}  
]  
}
```

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{  
  "error": {  
    "arguments": [  
      {  
        "code": "string",  
        "message": "string"  
      }  
    ],  
    "code": "4",  
    "message": "entry doesn't exist",  
    "target": "uuid"  
  }  
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

collection_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

policies

Name	Type	Description
_links	_links	
name	string	Specifies the name of the policy. A policy name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

users

Name	Type	Description
_links	_links	
name	string	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".

s3_group

This is a container for S3 user groups.

Name	Type	Description
comment	string	Can contain any additional information about the group being created or modified.
id	integer	Specifies a unique Group ID used to identify a particular group. This parameter should not be specified in the POST or PATCH method. A Group ID is automatically generated and it is retrieved using the GET method. Group ID is SVM-scoped.
name	string	Specifies the name of the group. A group name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".
policies	array[policies]	Specifies a list of policies that are attached to the group. The wildcard character "*" is a valid value for specifying all policies.
svm	svm	SVM, applies only to SVM-scoped objects.
users	array[users]	Specifies the list of users who belong to the group.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create an S3 group configuration

POST /protocols/s3/services/{svm.uuid}/groups

Introduced In: 9.8

Creates the S3 group configuration.

Important notes

- Each SVM can have one or more s3 group configurations.

Required properties

- `svm.uuid` - Existing SVM in which to create the user configuration.
- `name` - Group name that is to be created.
- `users` - List of users to be added into the group.
- `policies` - List of policies are to be attached to this group.

Recommended optional properties

- `comment` - Short description about the S3 Group.

Related ONTAP commands

- `vserver object-store-server group create`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/groups](#)

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
comment	string	Can contain any additional information about the group being created or modified.
id	integer	Specifies a unique Group ID used to identify a particular group. This parameter should not be specified in the POST or PATCH method. A Group ID is automatically generated and it is retrieved using the GET method. Group ID is SVM-scoped.
name	string	Specifies the name of the group. A group name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ";", ":", "@", and "-".
policies	array[policies]	Specifies a list of policies that are attached to the group. The wildcard character "*" is a valid value for specifying all policies.
svm	svm	SVM, applies only to SVM-scoped objects.

Name	Type	Description
users	array[users]	Specifies the list of users who belong to the group.

Example request

```
{
  "comment": "Admin group",
  "id": 5,
  "name": "Admin-Group",
  "policies": [
    {
      "name": "Policy1"
    }
  ],
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "users": [
    {
      "name": "user-1"
    }
  ]
}
```

Response

Status: 201, Created

Name	Type	Description
num_records	integer	Number of records
records	array[s3_group]	

Example response

```
{
  "num_records": 1,
  "records": [
    {
      "comment": "Admin group",
      "id": 5,
      "name": "Admin-Group",
      "policies": [
        {
          "name": "Policy1"
        }
      ],
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "users": [
        {
          "name": "user-1"
        }
      ]
    }
  ]
}
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
92405896	Users list cannot be empty.
92405930	Group name "{group name}" is not valid. Group names must have between 1 and 128 characters.

Error Code	Description
92405931	Group name "{group name}" contains invalid characters. Valid characters for a group name are 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".
92405932	Creating an object store group requires an effective cluster version of 9.8 or later.
92405933	Failed to create group for SVM. Reason: "{reason of failure}".
92405934	Users {user name} specified in the user list do not exist for SVM "{vserver name}". Use the "object-store-server user create" command to create a user.
92405935	Internal Error. Unable to generate unique ID for the group.
92405936	Query characters such as * are not supported in the user list.
92405937	Policies {policy name} specified in the policy list do not exist for SVM "{vserver name}".
92405942	Group name "{group name}" already exists for SVM "{vserver name}".
92405858	Failed to "create" the "group" because the operation is only supported on data SVMs.
262222	User name is present more than once in the users field.
92406154	Users {user} specified in the user list do not exist for SVM "vs1". Use the "/protocols/s3/services/{svm.uuid}/users" endpoint to create a user.
92406307	Cannot add object store user "user1" in SVM "vs1" to the group. Reason: The user is disabled, because it does not have keys generated.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

policies

Name	Type	Description
name	string	Specifies the name of the policy. A policy name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

users

Name	Type	Description
name	string	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".

s3_group

This is a container for S3 user groups.

Name	Type	Description
comment	string	Can contain any additional information about the group being created or modified.
id	integer	Specifies a unique Group ID used to identify a particular group. This parameter should not be specified in the POST or PATCH method. A Group ID is automatically generated and it is retrieved using the GET method. Group ID is SVM-scoped.
name	string	Specifies the name of the group. A group name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".
policies	array[policies]	Specifies a list of policies that are attached to the group. The wildcard character "*" is a valid value for specifying all policies.
svm	svm	SVM, applies only to SVM-scoped objects.
users	array[users]	Specifies the list of users who belong to the group.

collection_links

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments

Name	Type	Description
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete an S3 group configuration for an SVM

DELETE /protocols/s3/services/{svm.uuid}/groups/{id}

Introduced In: 9.8

Deletes the S3 group configuration of an SVM.

Related ONTAP commands

- `vserver object-store-server group delete`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/groups](#)

Parameters

Name	Type	In	Required	Description
id	string	path	True	Group identifier that identifies the unique group.
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Response

Status: 200, Ok

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve an S3 group configuration for an SVM

GET /protocols/s3/services/{svm.uuid}/groups/{id}

Introduced In: 9.8

Retrieves the S3 group configuration of an SVM.

Related ONTAP commands

- `vserver object-store-server group show`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/groups](#)

Parameters

Name	Type	In	Required	Description
id	string	path	True	Group identifier that identifies the unique group.
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.

Response

Status: 200, Ok

Name	Type	Description
comment	string	Can contain any additional information about the group being created or modified.
id	integer	Specifies a unique Group ID used to identify a particular group. This parameter should not be specified in the POST or PATCH method. A Group ID is automatically generated and it is retrieved using the GET method. Group ID is SVM-scoped.

Name	Type	Description
name	string	Specifies the name of the group. A group name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ";", ":", "@", and "-".
policies	array[policies]	Specifies a list of policies that are attached to the group. The wildcard character "*" is a valid value for specifying all policies.
svm	svm	SVM, applies only to SVM-scoped objects.
users	array[users]	Specifies the list of users who belong to the group.

Example response

```
{
  "comment": "Admin group",
  "id": 5,
  "name": "Admin-Group",
  "policies": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "Policy1"
    }
  ],
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "users": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1"
    }
  ]
}
```

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

policies

Name	Type	Description
_links	_links	
name	string	Specifies the name of the policy. A policy name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

users

Name	Type	Description
_links	_links	

Name	Type	Description
name	string	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update an S3 group configuration for an SVM

PATCH /protocols/s3/services/{svm.uuid}/groups/{id}

Introduced In: 9.8

Updates the S3 group configuration of an SVM.

Important notes

- The following fields can be modified for a group:
- `name` - Group name that needs to be modified.
- `users` - List of users present in the group.
- `policies` - List of policies to be attached to this group.

Recommended optional properties

- `comment` - Short description about the S3 Group.

Related ONTAP commands

- `vserver object-store-server group modify`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/groups](#)

Parameters

Name	Type	In	Required	Description
id	integer	path	True	Group identifier that identifies the unique group.
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
comment	string	Can contain any additional information about the group being created or modified.
id	integer	Specifies a unique Group ID used to identify a particular group. This parameter should not be specified in the POST or PATCH method. A Group ID is automatically generated and it is retrieved using the GET method. Group ID is SVM-scoped.
name	string	Specifies the name of the group. A group name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ":", "@", and "-".

Name	Type	Description
policies	array[policies]	Specifies a list of policies that are attached to the group. The wildcard character "*" is a valid value for specifying all policies.
svm	svm	SVM, applies only to SVM-scoped objects.
users	array[users]	Specifies the list of users who belong to the group.

Example request

```
{
  "comment": "Admin group",
  "id": 5,
  "name": "Admin-Group",
  "policies": [
    {
      "name": "Policy1"
    }
  ],
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "users": [
    {
      "name": "user-1"
    }
  ]
}
```

Response

Status: 200, Ok

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
92405896	Users list cannot be empty.
92405930	Group name "{group name}" is not valid. Group names must have between 1 and 128 characters.
92405931	Group name "{group name}" contains invalid characters. Valid characters for a group name are 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".
92405934	Users {user name} specified in the user list do not exist for SVM "{vserver name}". Use the "object-store-server user create" command to create a user.
92405936	Query characters such as * are not supported in the user list.
92405937	Policies {policy name} specified in the policy list do not exist for SVM "{vserver name}".
262222	User name is present more than once in the users field.
2621706	The specified "{svm.uuid}" and "{svm.name}" refer to different SVMs.
92406154	Users {user} specified in the user list do not exist for SVM "vs1". Use the "/protocols/s3/services/{svm.uuid}/users" endpoint to create a user.
92406307	Cannot add object store user "user1" in SVM "vs1" to the group. Reason: The user is disabled, because it does not have keys generated.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

policies

Name	Type	Description
name	string	Specifies the name of the policy. A policy name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

users

Name	Type	Description
name	string	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".

s3_group

This is a container for S3 user groups.

Name	Type	Description
comment	string	Can contain any additional information about the group being created or modified.
id	integer	Specifies a unique Group ID used to identify a particular group. This parameter should not be specified in the POST or PATCH method. A Group ID is automatically generated and it is retrieved using the GET method. Group ID is SVM-scoped.
name	string	Specifies the name of the group. A group name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".
policies	array[policies]	Specifies a list of policies that are attached to the group. The wildcard character "*" is a valid value for specifying all policies.
svm	svm	SVM, applies only to SVM-scoped objects.
users	array[users]	Specifies the list of users who belong to the group.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve S3 protocol historical performance metrics

GET /protocols/s3/services/{svm.uuid}/metrics

Introduced In: 9.8

Retrieves historical performance metrics for the S3 protocol of an SVM.

Parameters

Name	Type	In	Required	Description
status	string	query	False	Filter by status
latency.other	integer	query	False	Filter by latency.other
latency.total	integer	query	False	Filter by latency.total
latency.read	integer	query	False	Filter by latency.read
latency.write	integer	query	False	Filter by latency.write
throughput.read	integer	query	False	Filter by throughput.read
throughput.total	integer	query	False	Filter by throughput.total
throughput.write	integer	query	False	Filter by throughput.write
timestamp	string	query	False	Filter by timestamp
duration	string	query	False	Filter by duration
iops.other	integer	query	False	Filter by iops.other

Name	Type	In	Required	Description
iops.total	integer	query	False	Filter by iops.total
iops.read	integer	query	False	Filter by iops.read
iops.write	integer	query	False	Filter by iops.write
svm.uuid	string	path	True	Unique identifier of the SVM.
interval	string	query	False	<p>The time range for the data. Examples can be 1h, 1d, 1m, 1w, 1y. The period for each time range is as follows:</p> <ul style="list-style-type: none"> • 1h: Metrics over the most recent hour sampled over 15 seconds. • 1d: Metrics over the most recent day sampled over 5 minutes. • 1w: Metrics over the most recent week sampled over 30 minutes. • 1m: Metrics over the most recent month sampled over 2 hours. • 1y: Metrics over the most recent year sampled over a day. • Default value: 1 • enum: ["1h", "1d", "1w", "1m", "1y"]

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.</p> <ul style="list-style-type: none"> • Default value: 15 • Max value: 120 • Min value: 0
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
order_by	array[string]	query	False	Order results by specified fields and optional [asc
desc] direction. Default direction is 'asc' for ascending.	return_records	boolean	query	False

Response

Status: 200, Ok

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[records]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "duration": "PT15S",
      "iops": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "latency": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "status": "ok",
      "throughput": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "timestamp": "2017-01-25 06:20:13 -0500"
    }
  ]
}
```

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
8586226	UUID not found.
8585947	There are no entries matching your query.

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

iops

The rate of I/O operations observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency

The round trip latency in microseconds observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput

The rate of throughput bytes per second observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

records

Performance numbers, such as IOPS latency and throughput.

Name	Type	Description
_links	_links	

Name	Type	Description
duration	string	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
iops	iops	The rate of I/O operations observed at the storage object.
latency	latency	The round trip latency in microseconds observed at the storage object.
status	string	Errors associated with the sample. For example, if the aggregation of data over multiple nodes fails, then any partial errors might return "ok" on success or "error" on an internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput	throughput	The rate of throughput bytes per second observed at the storage object.
timestamp	string	The timestamp of the performance data.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage S3 service policies

Manage S3 service policies

Overview

An S3 policy is an object that when associated with a resource, defines their permissions. Buckets and objects are defined as resources. Policies are used to manage access to these resources.

Examples

Retrieving all fields for all S3 policies of an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/policies:

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-0050568ea123/policies?fields=*&return_records=true&return_timeout=15" -H "accept: application/json"

# The response:
{
  "num_records": 2,
  "records": [
    {
```

```

"comment": "S3 policy.",
"name": "Policy1",
"statements": [
  {
    "actions": [
      "*"
    ],
    "effect": "allow",
    "index": 0,
    "resources": [
      "bucket1",
      "bucket1/*"
    ],
    "sid": "FullAccessToBucket1"
  },
  {
    "actions": [
      "DeleteObject"
    ],
    "effect": "deny",
    "index": 1,
    "resources": [
      "*"
    ],
    "sid": "DenyDeleteObjectAccessToAllResources"
  }
],
"svm": {
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
{
  "comment": "S3 policy 2.",
  "name": "Policy2",
  "statements": [
    {
      "actions": [
        "GetObject"
      ],
      "effect": "allow",
      "index": 3,
      "resources": [
        "*"
      ],
      "sid": "AllowGetObjectAccessToAllResources"
    }
  ]
}

```

```
    },
    {
      "actions": [
        "*"
      ],
      "effect": "deny",
      "index": 3,
      "resources": [
        "*"
      ],
      "sid": "DenyAccessToAllResources"
    }
  ],
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
}
]
```

Retrieving the specified policy in the SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/policies/{name}:

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-0050568ea123/policies/Policy1?fields=*" -H "accept: application/json"

# The response:
{
  "comment": "S3 policy.",
  "name": "Policy1",
  "statements": [
    {
      "actions": [
        "GetObject",
        "PutObject",
        "DeleteObject",
        "ListBucket",
        "ListMyBuckets",
        "ListBucketMultipartUploads",
        "ListMultipartUploadParts",
        "GetObjectTagging",
        "PutObjectTagging",
        "DeleteObjectTagging",
        "GetBucketVersioning",
        "PutBucketVersioning"
      ],
      "effect": "deny",
      "index": 0,
      "resources": [
        "*"
      ],
      "sid": "DenyAccessToAllResources"
    }
  ],
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Creating an S3 policy for an SVM

```
# The API:
```

```
/api/protocols/s3/services/{svm.uuid}/policies
```

```
# The call:
```

```
curl -X POST "https://<mgmt-ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-0050568eal23/policies?return_records=true" -H "accept: application/json" -H "authorization: Basic <CREDENTIALS>" -H "Content-Type: application/json" -d "{ \"comment\": \"S3 policy.\", \"name\": \"Policy1\", \"statements\": [ { \"actions\": [ \"ListBucket\", \"ListMyBuckets\", \"CreateBucket\", \"DeleteBucket\" ], \"effect\": \"allow\", \"resources\": [ \"*\" ], \"sid\": \"AllowListAccessToAllResources\" } ] }"
```

```
# The response:
```

```
HTTP/1.1 202 Accepted
Date: Mon, 16 Mar 2020 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 289
Content-Type: application/json
{
  "num_records": 1,
  "records": [
    {
      "comment": "S3 policy.",
      "name": "Policy1",
      "statements": [
        {
          "actions": [
            "ListBucket",
            "ListMyBuckets"
          ],
          "effect": "allow",
          "index": 5,
          "resources": [
            "*"
          ],
          "sid": "AllowListAccessToAllResources"
        }
      ],
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```

```
}
```

Updating an S3 policy for an SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/policies/{name}:

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-0050568ea123/policies/Policy1" -H "accept: application/json" -H "authorization: Basic <CREDENTIALS>" -H "Content-Type: application/json" -d "{ \"comment\": \"S3 policy.\", \"statements\": [ { \"actions\": [ \"GetObject\", \"PutObject\", \"DeleteObject\", \"ListBucket\", \"ListMyBuckets\", \"CreateBucket\", \"DeleteBucket\" ], \"effect\": \"allow\", \"resources\": [ \"bucket1\", \"bucket1/*\" ], \"sid\": \"FullAccessToAllResources\" } ] }"

# The response:
HTTP/1.1 202 Accepted
Date: Mon, 16 Mar 2020 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
```

Deleting an S3 policy for a specified SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/policies/{name}:

# The call:
curl -X DELETE "https://<mgmt-ip>/api/protocols/s3/services/12f3ba4c-7ae0-11e9-8c06-0050568ea123/policies/Policy1" -H "accept: application/json"

# The response:
HTTP/1.1 202 Accepted
Date: Mon, 16 Mar 2020 11:32:27 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 189
Content-Type: application/json
```


Retrieve the S3 policies in an SVM configuration

GET /protocols/s3/services/{svm.uuid}/policies

Introduced In: 9.8

Retrieves the S3 policies SVM configuration.

Related ONTAP commands

- `vserver object-store-server policy show`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/policies](#)

Parameters

Name	Type	In	Required	Description
comment	string	query	False	Filter by comment <ul style="list-style-type: none">• maxLength: 256• minLength: 0
name	string	query	False	Filter by name <ul style="list-style-type: none">• maxLength: 128• minLength: 1
statements.sid	string	query	False	Filter by statements.sid <ul style="list-style-type: none">• maxLength: 256• minLength: 0
statements.index	integer	query	False	Filter by statements.index
statements.effect	string	query	False	Filter by statements.effect
statements.actions	string	query	False	Filter by statements.actions
statements.resources	string	query	False	Filter by statements.resources

Name	Type	In	Required	Description
read-only	boolean	query	False	Filter by read-only
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	<p>The default is true for GET calls. When set to false, only the number of records is returned.</p> <ul style="list-style-type: none"> • Default value: 1
return_timeout	integer	query	False	<p>The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.</p> <ul style="list-style-type: none"> • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

Status: 200, Ok

Name	Type	Description
_links	collection_links	
num_records	integer	Number of records
records	array[s3_policy]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "comment": "S3 policy.",
      "name": "Policy1",
      "statements": [
        {
          "actions": [
            "*"
          ],
          "effect": "allow",
          "index": 0,
          "resources": [
            "bucket1",
            "bucket1/*"
          ],
          "sid": "FullAccessToBucket1"
        }
      ],
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

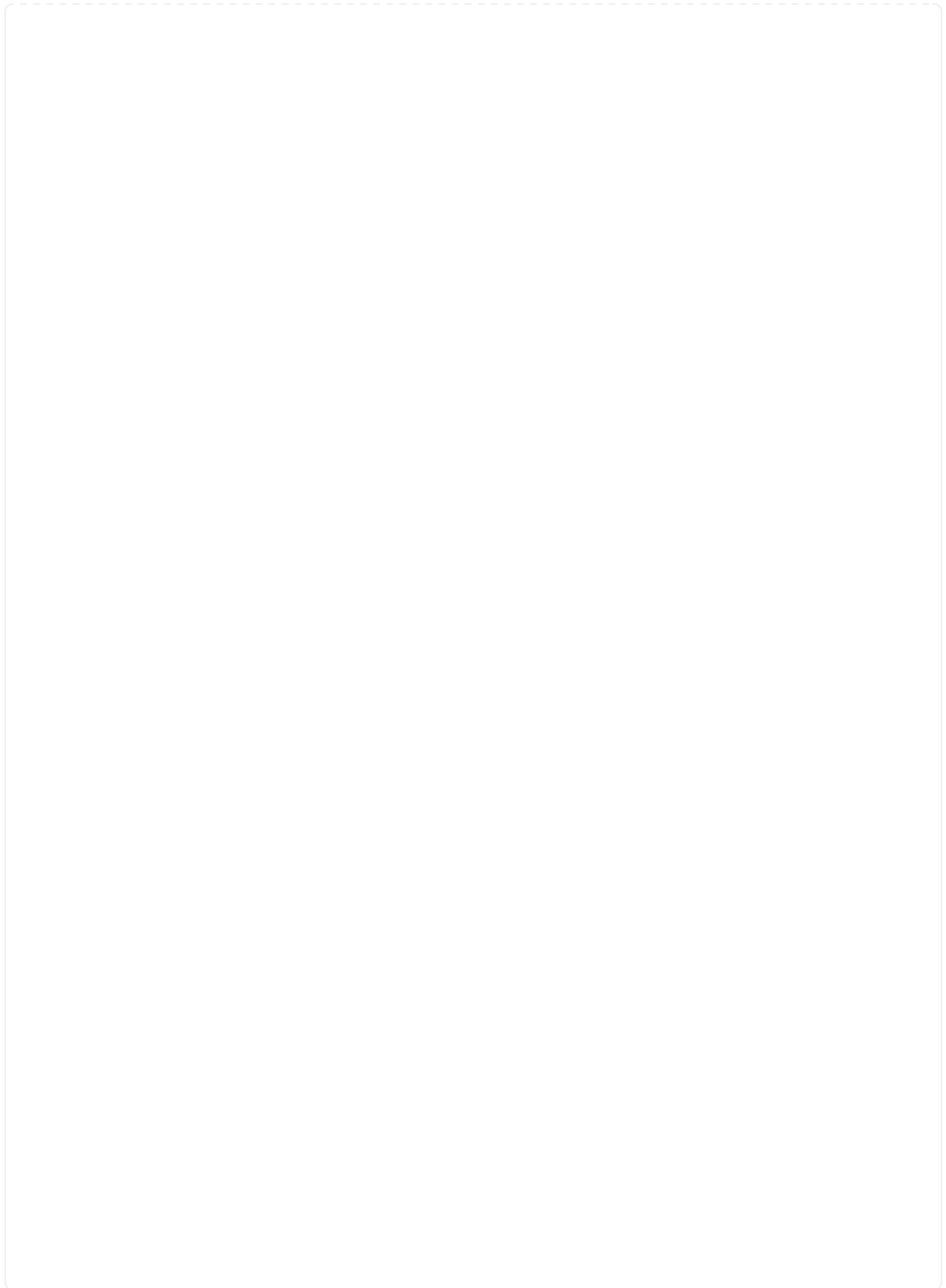
Name	Type	Description
href	string	

collection_links

Name	Type	Description
next	href	
self	href	

s3_policy_statement

Specifies information about a single access policy statement.



Name	Type	Description
actions	array[string]	<p>For each resource, S3 supports a set of operations. The resource operations allowed or denied are identified by an action list:</p> <ul style="list-style-type: none"> • GetObject - retrieves objects from a bucket. • PutObject - puts objects in a bucket. • DeleteObject - deletes objects from a bucket. • ListBucket - lists the objects in a bucket. • GetBucketAcl - retrieves the access control list (ACL) of a bucket. • GetObjectAcl - retrieves the access control list (ACL) of an object. • ListAllMyBuckets - lists all of the buckets in a server. • ListBucketMultipartUploads - lists the multipart uploads in progress for a bucket. • ListMultipartUploadParts - lists the parts in a multipart upload. • CreateBucket - creates a new bucket. • DeleteBucket - deletes an existing bucket. • GetObjectTagging - retrieves the tag set of an object. • PutObjecttagging - sets the tag set for an object. • DeleteObjectTagging - deletes the tag set of an object. • GetBucketLocation - retrieves the location of a bucket. • GetBucketVersioning - retrieves the versioning configuration of a bucket. • PutBucketVersioning - modifies the versioning configuration of a bucket. • ListBucketVersions - lists the object versions in a bucket.

Name	Type	Description
effect	string	Specifies whether access is allowed or denied. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
index	integer	Specifies a unique statement index used to identify a particular statement. This parameter should not be specified in the POST method. A statement index is automatically generated. It is not retrieved in the GET method.
resources	array[string]	
sid	string	Specifies the statement identifier which contains additional information about the statement.

[_links](#)

Name	Type	Description
self	href	

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

s3_policy

An S3 policy is an object. It defines resource (bucket, folder or object) permissions. These policies get evaluated when an object store user makes a request. Permissions in the policies determine

whether the request is allowed or denied.

Name	Type	Description
comment	string	Can contain any additional information about the S3 policy.
name	string	Specifies the name of the policy. A policy name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-". It cannot be specified in a PATCH method.
read-only	boolean	Specifies whether or not the s3 policy is read only. This parameter should not be specified in the POST method.
statements	array[s3_policy_statement]	Specifies the policy statements.
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create an S3 policy configuration

POST /protocols/s3/services/{svm.uuid}/policies

Introduced In: 9.8

Creates the S3 policy configuration.

Important notes

- Each SVM can have one or more s3 policy configurations.

Required properties

- `svm.uuid` - Existing SVM in which to create the s3 policy configuration.
- `name` - Policy name that is to be created.

Recommended optional properties

- `comment` - Short description about the S3 policy.
- `statements.effect` - Indicates whether to allow or deny access.
- `statements.actions` - List of actions that can be allowed or denied access. Example: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `ListMyBuckets`, `ListBucketMultipartUploads`, `ListMultipartUploadParts`, `CreateBucket`, `DeleteBucket`, `GetObjectTagging`, `PutObjectTagging`, `DeleteObjectTagging`, `GetBucketVersioning`, `PutBucketVersioning`.
- `statements.resources` - Buckets or objects that can be allowed or denied access.
- `statements.sid` - Statement identifier providing additional information about the statement.

Related ONTAP commands

- `vserver object-store-server policy create`
- `vserver object-store-server policy add-statement`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/policies](#)

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. <ul style="list-style-type: none">• Default value:

Name	Type	In	Required	Description
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
comment	string	Can contain any additional information about the S3 policy.
name	string	Specifies the name of the policy. A policy name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-". It cannot be specified in a PATCH method.
read-only	boolean	Specifies whether or not the s3 policy is read only. This parameter should not be specified in the POST method.
statements	array[s3_policy_statement]	Specifies the policy statements.
svm	svm	SVM, applies only to SVM-scoped objects.

Example request

```
{
  "comment": "S3 policy.",
  "name": "Policy1",
  "statements": [
    {
      "actions": [
        "*"
      ],
      "effect": "allow",
      "index": 0,
      "resources": [
        "bucket1",
        "bucket1/*"
      ],
      "sid": "FullAccessToBucket1"
    }
  ],
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Response

Status: 201, Created

Name	Type	Description
num_records	integer	Number of records
records	array[s3_policy]	

Example response

```
{
  "num_records": 1,
  "records": [
    {
      "comment": "S3 policy.",
      "name": "Policy1",
      "statements": [
        {
          "actions": [
            "*"
          ],
          "effect": "allow",
          "index": 0,
          "resources": [
            "bucket1",
            "bucket1/*"
          ],
          "sid": "FullAccessToBucket1"
        }
      ],
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
92405906	The specified action name is invalid.
92405947	Creating an object store server policy or statement requires an effective cluster version of 9.8 or later.
92405948	Policy name is not valid. Policy names must have between 1 and 128 characters.
92405949	Policy name contains invalid characters. Valid characters: 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".
92405950	Policy name already exists for SVM.
92405954	Policy name is reserved for read-only policies. Cannot be used for custom policy creation.
92405963	Failed to create policy statements for policy. Reason: "{reason of failure}". Resolve all issues and retry the operation.
92405863	Failed to create s3 policy statements. Reason: "{reason of failure}". Valid ways to specify a resource are "__", "<bucket-name>", "<bucket-name>/.../...". Resolve all the issues and retry the operation. //end row

|Name |Type |Description

|actions |array[string] a|For each resource, S3 supports a set of operations. The resource operations allowed or denied are identified by an action list:

- GetObject - retrieves objects from a bucket.
- PutObject - puts objects in a bucket.
- DeleteObject - deletes objects from a bucket.
- ListBucket - lists the objects in a bucket.
- GetBucketAcl - retrieves the access control list (ACL) of a bucket.
- GetObjectAcl - retrieves the access control list (ACL) of an object.
- ListAllMyBuckets - lists all of the buckets in a server.
- ListBucketMultipartUploads - lists the multipart uploads in progress for a bucket.
- ListMultipartUploadParts - lists the parts in a multipart upload.
- CreateBucket - creates a new bucket.
- DeleteBucket - deletes an existing bucket.
- GetObjectTagging - retrieves the tag set of an object.
- PutObjecttagging - sets the tag set for an object.
- DeleteObjectTagging - deletes the tag set of an object.
- GetBucketLocation - retrieves the location of a bucket.
- GetBucketVersioning - retrieves the versioning configuration of a bucket.

- PutBucketVersioning - modifies the versioning configuration of a bucket.
- ListBucketVersions - lists the object versions in a bucket.
- PutBucketPolicy - puts bucket policy on the bucket specified.
- GetBucketPolicy - retrieves the bucket policy of a bucket.
- DeleteBucketPolicy - deletes the policy created for a bucket. The wildcard character "*" can be used to form a regular expression for specifying actions.

|effect |string a|Specifies whether access is allowed or denied. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.

|index |integer a|Specifies a unique statement index used to identify a particular statement. This parameter should not be specified in the POST method. A statement index is automatically generated. It is not retrieved in the GET method.

|resources |array|string a|

|sid |string a|Specifies the statement identifier which contains additional information about the statement.

[#href] [.api-collapsible-fifth-title] href

[cols=3*,options=header]

|Name |Type |Description

|href |string a|

[#_links] [.api-collapsible-fifth-title] _links [#svm] [.api-collapsible-fifth-title] svm

SVM, applies only to SVM-scoped objects.

[cols=3*,options=header]

|Name |Type |Description

|name |string a|The name of the SVM. This field cannot be specified in a PATCH method.

|uuid |string a|The unique identifier of the SVM. This field cannot be specified in a PATCH method.

[#s3_policy] [.api-collapsible-fifth-title] s3_policy

An S3 policy is an object. It defines resource (bucket, folder or object) permissions. These policies get evaluated when an object store user makes a request. Permissions in the policies determine whether the request is allowed or denied.

[cols=3*,options=header]

|Name |Type |Description

|comment |string a|Can contain any additional information about the S3 policy.

|name |string a|Specifies the name of the policy. A policy name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-". It cannot be specified in a PATCH method.

|read-only |boolean a|Specifies whether or not the s3 policy is read only. This parameter should not be specified in the POST method.

|statements |array[s3_policy_statement] a|Specifies the policy statements.

|svm |svm a|SVM, applies only to SVM-scoped objects.

```
[#collection_links] [.api-collapsible-fifth-title] collection_links [#error_arguments] [.api-collapsible-fifth-title] error_arguments
```

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

code	string a	Argument code
------	----------	---------------

message	string a	Message argument
---------	----------	------------------

```
[#returned_error] [.api-collapsible-fifth-title] returned_error
```

```
[cols=3*,options=header]
```

Name	Type	Description
------	------	-------------

arguments	array[error_arguments] a	Message arguments
-----------	--------------------------	-------------------

code	string a	Error code
------	----------	------------

message	string a	Error message
---------	----------	---------------

target	string a	The target parameter that caused the error.
--------	----------	---

=====

= Delete an S3 policy configuration

DELETE /protocols/s3/services/{svm.uuid}/policies/{name}

Introduced In: 9.8

Deletes the S3 policy configuration of an SVM.

== Related ONTAP commands

* vserver object-store-server policy delete * vserver object-store-server policy delete-statement

== Learn more

* [DOC /protocols/s3/services/{svm.uuid}/policies](#)

== Parameters

[cols=5*,options=header]

Name	Type	In	Required	Description
------	------	----	----------	-------------

name	string	path	True a	Policy name
------	--------	------	--------	-------------

svm.uuid	string	path	True a	UUID of the SVM to which this object belongs.
----------	--------	------	--------	---

== Response

` Status: 200, Ok `

== Error

` Status: Default `

ONTAP Error Response Codes [cols=2*,options=header]

Error Code	Description
------------	-------------

92405858	Failed to "delete" the "policy" because the operation is only supported on data SVMs.
----------	---

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

error	returned_error	a
-------	--------------------------------	---

.Example error [%collapsible%closed] ===== [source,json,subs==+macros] { "error": { "arguments": [{ "code": "string", "message": "string" }], "code": "4", "message": "entry doesn't exist", "target": "uuid" } } =====

== Definitions

[.api-def-first-level] .See Definitions [%collapsible%closed] ===== [#error_arguments] [.api-collapsible-fifth-title] error_arguments

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

code	string a	Argument code
------	----------	---------------

message	string a	Message argument
---------	----------	------------------

[#returned_error] [.api-collapsible-fifth-title] returned_error

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

arguments	array[error_arguments] a	Message arguments
-----------	--	-------------------

code	string a	Error code
------	----------	------------

message	string a	Error message
---------	----------	---------------

target	string a	The target parameter that caused the error.
--------	----------	---

=====

= Retrieve an S3 policy configuration

GET /protocols/s3/services/{svm.uuid}/policies/{name}

Introduced In: 9.8

Retrieves the S3 policy configuration of an SVM.

== Related ONTAP commands

* vserver object-store-server policy show

== Learn more

* [DOC /protocols/s3/services/{svm.uuid}/policies](#)

== Parameters

[cols=5*,options=header]

Name	Type	In	Required	Description
------	------	----	----------	-------------

|name |string |path |True a|Policy name

|svm.uuid |string |path |True a|UUID of the SVM to which this object belongs.

|fields |array|string| |query |False a|Specify the fields to return.

== Response

```
` Status: 200, Ok `
```

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

comment	string a	Can contain any additional information about the S3 policy.
---------	----------	---

name	string a	Specifies the name of the policy. A policy name length can range from 1 to 128 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-". It cannot be specified in a PATCH method.
------	----------	--

read-only	boolean a	Specifies whether or not the s3 policy is read only. This parameter should not be specified in the POST method.
-----------	-----------	---

statements	array s3_policy_statement a	Specifies the policy statements.
------------	--	----------------------------------

svm	svm a	SVM, applies only to SVM-scoped objects.
-----	-----------------------	--

.Example response [%collapsible%closed] ===== [source,json,subs=+macros] { "comment": "S3 policy.", "name": "Policy1", "statements": [{ "actions": [""], "effect": "allow", "index": 0, "resources": ["bucket1", "bucket1/"], "sid": "FullAccessToBucket1" }], "svm": { "_links": { "self": { "href": "/api/resourceLink" } }, "name": "svm1", "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7" } } =====

== Error

```
` Status: Default, Error `
```

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

error	returned_error a	
-------	----------------------------------	--

.Example error [%collapsible%closed] ===== [source,json,subs=+macros] { "error": { "arguments": [{ "code": "string", "message": "string" }], "code": "4", "message": "entry doesn't exist", "target": "uuid" } } =====

== Definitions

[.api-def-first-level] .See Definitions [%collapsible%closed] ===== [[s3_policy_statement](#)] [.api-collapsible-fifth-title] [s3_policy_statement](#)

Specifies information about a single access policy statement.

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

actions	array[string] a	For each resource, S3 supports a set of operations. The resource operations allowed or denied are identified by an action list:
---------	-----------------	---

- `GetObject` - retrieves objects from a bucket.
- `PutObject` - puts objects in a bucket.
- `DeleteObject` - deletes objects from a bucket.
- `ListBucket` - lists the objects in a bucket.
- `GetBucketAcl` - retrieves the access control list (ACL) of a bucket.
- `GetObjectAcl` - retrieves the access control list (ACL) of an object.
- `ListAllMyBuckets` - lists all of the buckets in a server.
- `ListBucketMultipartUploads` - lists the multipart uploads in progress for a bucket.
- `ListMultipartUploadParts` - lists the parts in a multipart upload.
- `CreateBucket` - creates a new bucket.
- `DeleteBucket` - deletes an existing bucket.
- `GetObjectTagging` - retrieves the tag set of an object.
- `PutObjecttagging` - sets the tag set for an object.
- `DeleteObjectTagging` - deletes the tag set of an object.
- `GetBucketLocation` - retrieves the location of a bucket.
- `GetBucketVersioning` - retrieves the versioning configuration of a bucket.
- `PutBucketVersioning` - modifies the versioning configuration of a bucket.
- `ListBucketVersions` - lists the object versions in a bucket.
- `PutBucketPolicy` - puts bucket policy on the bucket specified.
- `GetBucketPolicy` - retrieves the bucket policy of a bucket.
- `DeleteBucketPolicy` - deletes the policy created for a bucket. The wildcard character "*" can be used to form a regular expression for specifying actions.

effect	string a	Specifies whether access is allowed or denied. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
--------	----------	---

index	integer a	Specifies a unique statement index used to identify a particular statement. This parameter should not be specified in the POST method. A statement index is automatically generated. It is not retrieved in the GET method.
-------	-----------	---

resources	array[string] a	
-----------	-----------------	--

sid	string a	Specifies the statement identifier which contains additional information about the statement.
-----	----------	---

[\[#href\] \[.api-collapsible-fifth-title\] href](#)

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

|href |string a|

```
[#_links] [.api-collapsible-fifth-title] _links  
[cols=3*,options=header]
```

|Name |Type |Description

|self |[href](#) a|

```
[#svm] [.api-collapsible-fifth-title] svm  
SVM, applies only to SVM-scoped objects.  
[cols=3*,options=header]
```

|Name |Type |Description

|_links |[_links](#) a|

|name |string a|The name of the SVM. This field cannot be specified in a PATCH method.

|uuid |string a|The unique identifier of the SVM. This field cannot be specified in a PATCH method.

```
[#error_arguments] [.api-collapsible-fifth-title] error_arguments  
[cols=3*,options=header]
```

|Name |Type |Description

|code |string a|Argument code

|message |string a|Message argument

```
[#returned_error] [.api-collapsible-fifth-title] returned_error  
[cols=3*,options=header]
```

|Name |Type |Description

|arguments |array[[error_arguments](#)] a|Message arguments

|code |string a|Error code

|message |string a|Error message

|target |string a|The target parameter that caused the error.

=====

= Update an S3 policy configuration

PATCH /protocols/s3/services/{svm.uuid}/policies/{name}

Introduced In: 9.8

Updates the S3 policy configuration of an SVM.

== Important notes

* The following fields can be modified for a policy:

* **comment** - Any information related to the policy.

* **statements** - Specifies the array of policy statements.

== Related ONTAP commands

* `vserver object-store-server policy modify` * `vserver object-store-server policy modify-statement`

== Learn more

* [DOC /protocols/s3/services/{svm.uuid}/policies](#)

== Parameters

[cols=5*,options=header]

Name	Type	In	Required	Description
------	------	----	----------	-------------

name	string	path	True	a Policy name
------	--------	------	------	---------------

svm.uuid	string	path	True	a UUID of the SVM to which this object belongs.
----------	--------	------	------	---

== Request Body

[cols=3*,options=header]

Name	Type	Description
------	------	-------------

comment	string	a Can contain any additional information about the S3 policy.
---------	--------	---

read-only	boolean	a Specifies whether or not the s3 policy is read only. This parameter should not be specified in the POST method.
-----------	---------	---

statements	array	[s3_policy_statement] a Specifies the policy statements.
------------	-------	--

svm	svm	a SVM, applies only to SVM-scoped objects.
-----	---------------------	--

```
.Example request [%collapsible%closed] ===== [source,json,subs=+macros] { "comment": "S3 policy.",
"statements": [ { "actions": [ "" ], "effect": "allow", "index": 0, "resources": [ "bucket1", "bucket1/" ], "sid":
"FullAccessToBucket1" } ], "svm": { "name": "svm1", "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7" } }
=====
```

== Response

```
` Status: 200, Ok `
```

== Error

```
` Status: Default `
```

ONTAP Error Response Codes [cols=2__,options=header]

Error Code	Description
92405906	The specified action name is invalid.
92405963	Failed to create s3 policy statements "{policy name}". Reason: "{reason of failure}". Resolve all issues and retry the operation.
92405953	Object store server read-only policies do not support create, modify, delete, add-statement, remove-statement and modify-statement operations.
92406075	Failed to modify policy statement for policy "{policy name}". Reason: "{reason of failure}". Valid ways to specify a resource are "___", "<bucket-name>", "<bucket-name>/.../...".

Definitions

See Definitions

s3_policy_statement

Specifies information about a single access policy statement.



Name	Type	Description
actions	array[string]	<p>For each resource, S3 supports a set of operations. The resource operations allowed or denied are identified by an action list:</p> <ul style="list-style-type: none"> • GetObject - retrieves objects from a bucket. • PutObject - puts objects in a bucket. • DeleteObject - deletes objects from a bucket. • ListBucket - lists the objects in a bucket. • GetBucketAcl - retrieves the access control list (ACL) of a bucket. • GetObjectAcl - retrieves the access control list (ACL) of an object. • ListAllMyBuckets - lists all of the buckets in a server. • ListBucketMultipartUploads - lists the multipart uploads in progress for a bucket. • ListMultipartUploadParts - lists the parts in a multipart upload. • CreateBucket - creates a new bucket. • DeleteBucket - deletes an existing bucket. • GetObjectTagging - retrieves the tag set of an object. • PutObjecttagging - sets the tag set for an object. • DeleteObjectTagging - deletes the tag set of an object. • GetBucketLocation - retrieves the location of a bucket. • GetBucketVersioning - retrieves the versioning configuration of a bucket. • PutBucketVersioning - modifies the versioning configuration of a bucket. • ListBucketVersions - lists the object versions in a bucket.

Name	Type	Description
effect	string	Specifies whether access is allowed or denied. If access (to allow) is not granted explicitly to a resource, access is implicitly denied. Access can also be denied explicitly to a resource, in order to make sure that a user cannot access it, even if a different policy grants access.
index	integer	Specifies a unique statement index used to identify a particular statement. This parameter should not be specified in the POST method. A statement index is automatically generated. It is not retrieved in the GET method.
resources	array[string]	
sid	string	Specifies the statement identifier which contains additional information about the statement.

href

Name	Type	Description
href	string	

_links

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

s3_policy

An S3 policy is an object. It defines resource (bucket, folder or object) permissions. These policies get evaluated when an object store user makes a request. Permissions in the policies determine

whether the request is allowed or denied.

Name	Type	Description
comment	string	Can contain any additional information about the S3 policy.
read-only	boolean	Specifies whether or not the s3 policy is read only. This parameter should not be specified in the POST method.
statements	array[s3_policy_statement]	Specifies the policy statements.
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Manage S3 service users

Manage S3 service users

Overview

An S3 user account is created on the S3 server. Buckets that are created for the server are associated with that user (as the owner of the buckets). The creation of the user account involves generating a pair of keys "access" and "secret". These keys are shared with clients (by the administrator out of band) who want to

access the S3 server. The `access_key` is sent in the request and it identifies the user performing the operation. The client or server never send the `secret_key` over the wire. Only the `access_key` can be retrieved from a GET operation. The `secret_key` along with the `access_key` is returned from a POST operation and from a PATCH operation if the administrator needs to regenerate the keys. If the user is part of active-directory, the user name takes the format "user@fully_qualified_domain_name".

Examples

Retrieving S3 user configurations for a particular SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/users

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users?fields=*&return_records=true" -H "accept: application/hal+json"

# The response:
{
  "records": [
    {
      "svm": {
        "uuid": "db2ec036-8375-11e9-99e1-0050568e3ed9",
        "name": "vs1",
        "_links": {
          "self": {
            "href": "/api/svm/svms/db2ec036-8375-11e9-99e1-0050568e3ed9"
          }
        }
      },
      "name": "user-1",
      "comment": "S3 user",
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "key_time_to_live": "PT3H5M",
      "key_expiry_time": "2023-11-13T23:28:03+05:30",
      "id": 3,
      "keys": [
        {
          "id": 1,
          "access_key": "<AWS-ACCESS-KEY-ID>",
          "time_to_live": "PT3H5M",
          "expiry_time": "2023-11-13T23:28:03+05:30"
        },
        {
          "id": 2,
          "access_key": "<AWS-ACCESS-KEY-ID>",
```

```

        "time_to_live": "PT6H3M2S",
        "expiry_time": "2023-11-13T23:24:41+05:30"
    }
],
"_links": {
    "self": {
        "href": "/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users/user-1"
    }
}
},
{
    "svm": {
        "uuid": "db2ec036-8375-11e9-99e1-0050568e3ed9",
        "name": "vs1",
        "_links": {
            "self": {
                "href": "/api/svm/svms/db2ec036-8375-11e9-99e1-0050568e3ed9"
            }
        }
    },
    "name": "user-2",
    "comment": "s3-user",
    "access_key": "<AWS-ACCESS-KEY-ID>",
    "id": 2,
    "keys": [
        {
            "id": 1,
            "access_key": "<AWS-ACCESS-KEY-ID>",
        }
    ],
    "_links": {
        "self": {
            "href": "/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users/user-2"
        }
    }
}
],
"num_records": 2,
"_links": {
    "self": {
        "href": "/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users?fields=*&return_records=true"
    }
}
}

```

```
}
```

Retrieving the user configuration of a specific S3 user


```

# The API:
/api/protocols/s3/services/{svm.uuid}/users/{name}

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users/user-1" -H "accept: application/hal+json"

# The response:
{
  "svm": {
    "uuid": "db2ec036-8375-11e9-99e1-0050568e3ed9",
    "name": "vs1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/db2ec036-8375-11e9-99e1-0050568e3ed9"
      }
    }
  },
  "name": "user-1",
  "comment": "s3-user",
  "access_key": "<AWS-ACCESS-KEY-ID>",
  "key_time_to_live": "P6DT1H5M",
  "key_expiry_time": "2023-02-20T10:04:31Z",
  "id": 3,
  "keys": [
    {
      "id": 1,
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "time_to_live": "PT3H5M",
      "expiry_time": "2023-11-13T23:28:03+05:30"
    },
    {
      "id": 2,
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "time_to_live": "PT6H3M2S",
      "expiry_time": "2023-11-13T23:24:41+05:30"
    }
  ],
  "_links": {
    "self": {
      "href": "/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users/user-1"
    }
  }
}

```

Creating an S3 user configuration

```
# The API:
/api/protocols/s3/services/{svm.uuid}/users

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users" -H "accept: application/json" -H "Content-Type: application/json" -d '{"name": "user-1"}'

# The response:
HTTP/1.1 201 Created
Date: Fri, 31 May 2019 09:34:25 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users/user-1
Content-Length: 244
Content-Type: application/json
{
  "num_records": 1,
  "records": [
    {
      "name": "user-1",
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "secret_key": "<AWS-SECRET-ACCESS-KEY>"
    }
  ]
}
```

Creating an S3 user configuration with key expiration configuration

```

# The API:
/api/protocols/s3/services/{svm.uuid}/users

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users" -H "accept: application/json" -H "Content-Type: application/json" -d '{"comment\":"S3 user3\","key_time_to_live\":"P6DT1H5M\","name\":"user-3\"}'

# The response:
HTTP/1.1 201 Created
Date: Tue, 14 Feb 2023 08:59:31 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self' data:; frame-ancestors: 'self'
Location: /api/protocols/s3/services/6573ac2b-ab66-11ed-b53d-005056bb4b9b/users/user-3
Content-Length: 337
Content-Type: application/hal+json
Vary: Origin
{
  "num_records": 1,
  "records": [
    {
      "name": "user-3",
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "secret_key": "<AWS-SECRET-ACCESS-KEY>",
      "key_expiry_time": "2023-06-16T12:08:38Z",
      "_links": {
        "self": {
          "href": "/api/protocols/s3/services/6573ac2b-ab66-11ed-b53d-005056bb4b9b/users/user-3"
        }
      }
    }
  ]
}

```

Creating an S3 user configuration with user keys specified

```

# The API:
/api/protocols/s3/services/{svm.uuid}/users

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users" -H "accept: application/json" -H "Content-Type: application/json" -d '{"access_key": "<AWS-ACCESS-KEY-ID>", "comment": "S3 user", "key_time_to_live": "PT6H3M", "name": "user-test", "secret_key": "<AWS-SECRET-ACCESS-KEY>"}'

# The response:
HTTP/1.1 201 Created
Date: Fri, 31 May 2019 09:34:25 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Location: /api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users/user-1
Content-Length: 244
Content-Type: application/json
{
  "num_records": 1,
  "records": [
    {
      "name": "user-test",
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "secret_key": "<AWS-SECRET-ACCESS-KEY>",
      "key_expiry_time": "2024-02-12T22:36:29+05:30"
    }
  ]
}

```

Creating an S3 user configuration with a key expiration configuration and where the user is part of Active directory.

```
# The API:
/api/protocols/s3/services/{svm.uuid}/users

# The call:
curl -X POST "https://<mgmt-ip>/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users" -H "accept: application/json" -H "Content-Type: application/json" -d '{"comment\":"S3 user3\","key_time_to_live\":"P6DT1H5M\","name\":"user-3@domain1.com\"}'

# The response:
HTTP/1.1 201 Created
Date: Tue, 14 Feb 2023 08:59:31 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self' data:; frame-ancestors: 'self'
Location: /api/protocols/s3/services/6573ac2b-ab66-11ed-b53d-005056bb4b9b/users/user-3%40domain1.com
Content-Length: 337
Content-Type: application/hal+json
Vary: Origin
{
  "num_records": 1,
  "records": [
    {
      "name": "user-3@domain1.com",
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "secret_key": "<AWS-SECRET-ACCESS-KEY>",
      "key_expiry_time": "2023-06-16T12:08:38Z",
      "_links": {
        "self": {
          "href": "/api/protocols/s3/services/6573ac2b-ab66-11ed-b53d-005056bb4b9b/users/user-3%40domain1.com"
        }
      }
    }
  ]
}
```

Regenerating first key for a specific S3 user for the specified SVM

```

# The API:
/api/protocols/s3/services/{svm.uuid}/users/{name}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users/user-2?regenerate_keys=true" -H "accept: application/hal+json" -H "Content-Type: application/json" -d "{}"

# The response:
HTTP/1.1 200 OK
Date: Fri, 31 May 2019 09:55:45 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 391
Content-Type: application/hal+json
{
  "num_records": 1,
  "records": [
    {
      "name": "user-2",
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "secret_key": "<AWS-SECRET-ACCESS-KEY>",
      "_links": {
        "self": {
          "href": "/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users/user-2"
        }
      }
    }
  ]
}

```

Regenerating keys and setting new expiry configuration for a specific S3 user for the specified SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/users/{name}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users/user-2?regenerate_keys=true" -H "accept: application/hal+json" -H "Content-Type: application/json" -d '{"key_time_to_live": "PT6H3M"}'

# The response:
HTTP/1.1 200 OK
Date: Fri, 31 May 2019 09:55:45 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 391
Content-Type: application/hal+json
{
  "num_records": 1,
  "records": [
    {
      "name": "user-2",
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "secret_key": "<>AWS-SECRET-ACCESS-KEY",
      "key_expiry_time": "2023-06-16T16:19:06Z",
      "_links": {
        "self": {
          "href": "/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users/user-2"
        }
      }
    }
  ]
}
```

Regenerating keys by specifying keys in the input

```
# The API:
/api/protocols/s3/services/{svm.uuid}/users/{name}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users/user-2?regenerate_keys=true" -H "accept: application/hal+json" -H "Content-Type: application/json" -d "{
  \"access_key\": \"<AWS-ACCESS-KEY-ID>\", \"comment\": \"S3 user\",
  \"key_time_to_live\": \"PT6H3M\", \"secret_key\": \"<AWS-SECRET-ACCESS-KEY>\"}"

# The response:
HTTP/1.1 200 OK
Date: Fri, 31 May 2019 09:55:45 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Length: 391
Content-Type: application/hal+json
{
  "num_records": 1,
  "records": [
    {
      "name": "user-2",
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "secret_key": "<AWS-SECRET-ACCESS-KEY>",
      "key_expiry_time": "2023-06-16T16:19:06Z",
      "_links": {
        "self": {
          "href": "/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users/user-2"
        }
      }
    }
  ]
}
```

Deleting first key for a specific S3 user for a specified SVM


```
# The API:
/api/protocols/s3/services/{svm.uuid}/users/{name}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/s3/services/db2ec036-8375-11e9-99e1-0050568e3ed9/users/user-2?delete_keys=true" -H "accept: application/hal+json" -H "Content-Type: application/json" -d "{}"

# The response:
HTTP/1.1 200 OK
Date: Wed, 08 Feb 2023 13:40:04 GMT
Server: libzapid-httpd
X-Content-Type-Options: nosniff
Cache-Control: no-cache,no-store,must-revalidate
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self' data:; frame-ancestors: 'self'
Content-Length: 3
Content-Type: application/hal+json
Vary: Origin
{
}
```

Deleting the specified S3 user configuration for a specified SVM

```
# The API:
/api/protocols/s3/services/{svm.uuid}/users/{name}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/protocols/s3/services/03ce5c36-f269-11e8-8852-0050568e5298/users/user-2" -H "accept: application/json"
```

Retrieve the SVM configuration for an S3 user

GET /protocols/s3/services/{svm.uuid}/users

Introduced In: 9.7

Retrieves the S3 user's SVM configuration.

Related ONTAP commands

- `vserver object-store-server user show`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/users](#)

Parameters

Name	Type	In	Required	Description
key_expiry_time	string	query	False	Filter by key_expiry_time <ul style="list-style-type: none">• Introduced in: 9.14
name	string	query	False	Filter by name <ul style="list-style-type: none">• maxLength: 64• minLength: 1
svm.name	string	query	False	Filter by svm.name
comment	string	query	False	Filter by comment <ul style="list-style-type: none">• maxLength: 256• minLength: 0
key_time_to_live	string	query	False	Filter by key_time_to_live <ul style="list-style-type: none">• Introduced in: 9.14
access_key	string	query	False	Filter by access_key
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

Status: 200, Ok

Name	Type	Description
_links	collection_links	
num_records	integer	Number of records
records	array[s3_user]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "comment": "S3 user",
      "key_expiry_time": "2023-12-31 19:00:00 -0500",
      "key_time_to_live": "PT6H3M",
      "name": "user-1",
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

collection_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

s3_user

This is a container of S3 users.

Name	Type	Description
access_key	string	Specifies the access key for the user.
comment	string	Can contain any additional information about the user being created or modified.

Name	Type	Description
key_expiry_time	string	Specifies the date and time after which keys expire and are no longer valid.
key_time_to_live	string	<p>Indicates the time period from when this parameter is specified:</p> <ul style="list-style-type: none"> • when creating or modifying a user or • when the user keys were last regenerated, after which the user keys expire and are no longer valid. • Valid format is: 'PnDTnHnMnS PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If the value specified is '0' seconds, then the keys won't expire.
name	string	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".
svm	svm	SVM, applies only to SVM-scoped objects.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments

Name	Type	Description
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create an S3 user configuration

POST /protocols/s3/services/{svm.uuid}/users

Introduced In: 9.7

Creates the S3 user configuration.

Important notes

- Each SVM can have one or more user configurations.
- If the user is a member of Active directory, the user name takes the format "user@FQDN". For example, "user1@domain1.com".
- If user creation is successful, a user access_key and secret_key is returned as part of the response.
- If user keys have expiry configuration, then "key_expiry_time" is also returned as part of the response.
- User access and secret keys can be specified in the input. If not specified, keys are generated automatically.

Required properties

- svm.uuid - Existing SVM in which to create the user configuration.
- name - User name that is to be created.

Default property values

- comment - ""

Related ONTAP commands

- vserver object-store-server user create

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/users](#)

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
access_key	string	Specifies the access key for the user.
comment	string	Can contain any additional information about the user being created or modified.
key_expiry_time	string	Specifies the date and time after which keys expire and are no longer valid.
key_time_to_live	string	Indicates the time period from when this parameter is specified: <ul style="list-style-type: none"> • when creating or modifying a user or • when the user keys were last regenerated, after which the user keys expire and are no longer valid. • Valid format is: 'PnDTnHnMnS PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If the value specified is '0' seconds, then the keys won't expire.

Name	Type	Description
name	string	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ":", "@", and "-".
secret_key	string	Specifies the secret key for the user.
svm	svm	SVM, applies only to SVM-scoped objects.

Example request

```
{
  "access_key": "<AWS-ACCESS-KEY-ID>",
  "comment": "S3 user",
  "key_expiry_time": "2023-12-31 19:00:00 -0500",
  "key_time_to_live": "PT6H3M",
  "name": "user-1",
  "secret_key": "<AWS-SECRET-ACCESS-KEY>",
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Response

Status: 201, Created

Name	Type	Description
num_records	integer	Number of records
records	array[s3_service_user_post_response]	

Example response

```
{
  "num_records": 1,
  "records": [
    {
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "key_expiry_time": "2023-12-31 19:00:00 -0500",
      "name": "user-1",
      "secret_key": "<AWS-SECRET-ACCESS-KEY>"
    }
  ]
}
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
92405787	User name "User#1" contains invalid characters. Valid characters for a user name are 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".
92405788	User name "User01234567890123456789012345678901234567890123456789012345678901234567890123456789012345" is not valid. User names must have between 1 and 64 characters.
92405791	Failed to create access-key and secret-key.
92405817	SVM "<non-data SVM="" name="">" is not a data SVM. Specify a data SVM.</non-data>
92406083	The maximum supported value for user key expiry configuration is "1095" days.
92406096	The user does not have permission to access the requested resource \"{0}\".

Error Code	Description
92406097	Internal error. The operation configuration is not correct.
92406196	The specified value for the "key_time_to_live" field cannot be greater than the maximum limit specified for the "max_key_time_to_live" field in the object store server.

| 92406197 | Object store user "user-2" must have a non-zero value for the "key_time_to_live" field because the maximum limit specified for the "max_key_time_to_live" field in the object store server is not zero. |
 92406200 | An object store user with the same access-key already exists. | | 92406201 | Missing access-key or secret-key. Either provide both of the keys or none. If not provided, keys are generated automatically. | |
 92406205 | The object store user access key contains invalid characters. Valid characters are 0-9 and A-Z. |

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

s3_user

This is a container of S3 users.

Name	Type	Description
access_key	string	Specifies the access key for the user.
comment	string	Can contain any additional information about the user being created or modified.
key_expiry_time	string	Specifies the date and time after which keys expire and are no longer valid.

Name	Type	Description
key_time_to_live	string	<p>Indicates the time period from when this parameter is specified:</p> <ul style="list-style-type: none"> • when creating or modifying a user or • when the user keys were last regenerated, after which the user keys expire and are no longer valid. • Valid format is: 'PnDTnHnMnSnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If the value specified is '0' seconds, then the keys won't expire.
name	string	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ",", ".", "@", and "-".
secret_key	string	Specifies the secret key for the user.
svm	svm	SVM, applies only to SVM-scoped objects.

collection_links

s3_service_user_post_response

Name	Type	Description
access_key	string	Specifies the access key for the user.
key_expiry_time	string	Specifies the date and time after which the keys expire and are no longer valid.
name	string	The name of the user.

Name	Type	Description
secret_key	string	Specifies the secret key for the user.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete an S3 user configuration

```
DELETE /protocols/s3/services/{svm.uuid}/users/{name}
```

Introduced In: 9.7

Deletes the S3 user configuration of an SVM.

Related ONTAP commands

- `vserver object-store-server user delete`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/users](#)

Parameters

Name	Type	In	Required	Description
name	string	path	True	User name

Name	Type	In	Required	Description
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Response

Status: 200, Ok

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve the S3 user configuration for an SVM

GET /protocols/s3/services/{svm.uuid}/users/{name}

Introduced In: 9.7

Retrieves the S3 user configuration of an SVM.

Related ONTAP commands

- `vserver object-store-server user show`

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/users](#)

Parameters

Name	Type	In	Required	Description
name	string	path	True	User name
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

Response

Status: 200, Ok

Name	Type	Description
access_key	string	Specifies the access key for the user.
comment	string	Can contain any additional information about the user being created or modified.
key_expiry_time	string	Specifies the date and time after which keys expire and are no longer valid.
key_time_to_live	string	<p>Indicates the time period from when this parameter is specified:</p> <ul style="list-style-type: none"> • when creating or modifying a user or • when the user keys were last regenerated, after which the user keys expire and are no longer valid. • Valid format is: 'PnDTnHnMnS PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If the value specified is '0' seconds, then the keys won't expire.
name	string	Specifies the name of the user. A user name length can range from 1 to 64 characters and can only contain the following combination of characters 0-9, A-Z, a-z, "_", "+", "=", ";", ":", "@", and "-".

Name	Type	Description
svm	svm	SVM, applies only to SVM-scoped objects.

Example response

```
{
  "access_key": "<AWS-ACCESS-KEY-ID>",
  "comment": "S3 user",
  "key_expiry_time": "2023-12-31 19:00:00 -0500",
  "key_time_to_live": "PT6H3M",
  "name": "user-1",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update an S3 user configuration

PATCH /protocols/s3/services/{svm.uuid}/users/{name}

Introduced In: 9.7

Updates the S3 user configuration of an SVM.

Important notes

- User access_key and secret_key pair can be regenerated using the PATCH operation.
- User access_key and secret_key is returned in a PATCH operation if the "regenerate_keys" field is specified as true.
- If "regenerate_keys" is true and user keys have expiry configuration, then "key_expiry_time" is also returned as part of response.
- User access_key and secret_key pair can be deleted using the PATCH operation.

Recommended optional properties

- regenerate_keys - Specifies if secret_key and access_key need to be regenerated.
- delete_keys - Specifies if secret_key and access_key need to be deleted.
- comment - Any information related to the S3 user.

Related ONTAP commands

- vserver object-store-server user show
- vserver object-store-server user regenerate-keys
- vserver object-store-server user delete-keys

Learn more

- [DOC /protocols/s3/services/{svm.uuid}/users](#)

Parameters

Name	Type	In	Required	Description
name	string	path	True	User name
regenerate_keys	boolean	query	False	Specifies whether or not to regenerate the user keys. <ul style="list-style-type: none">• Default value:

Name	Type	In	Required	Description
delete_keys	boolean	query	False	Specifies whether or not to delete the user keys. <ul style="list-style-type: none"> Introduced in: 9.14 Default value:
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
access_key	string	Specifies the access key for the user.
comment	string	Can contain any additional information about the user being created or modified.
key_expiry_time	string	Specifies the date and time after which keys expire and are no longer valid.
key_time_to_live	string	Indicates the time period from when this parameter is specified: <ul style="list-style-type: none"> when creating or modifying a user or when the user keys were last regenerated, after which the user keys expire and are no longer valid. Valid format is: 'PnDTnHnMnS PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. If the value specified is '0' seconds, then the keys won't expire.

Name	Type	Description
secret_key	string	Specifies the secret key for the user.
svm	svm	SVM, applies only to SVM-scoped objects.

Example request

```
{
  "access_key": "<AWS-ACCESS-KEY-ID>",
  "comment": "S3 user",
  "key_expiry_time": "2023-12-31 19:00:00 -0500",
  "key_time_to_live": "PT6H3M",
  "secret_key": "<AWS-SECRET-ACCESS-KEY>",
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Response

Status: 200, Ok

Name	Type	Description
num_records	integer	Number of records
records	array[s3_service_user_post_respo nse]	

Example response

```
{
  "num_records": 1,
  "records": [
    {
      "access_key": "<AWS-ACCESS-KEY-ID>",
      "key_expiry_time": "2023-12-31 19:00:00 -0500",
      "name": "user-1",
      "secret_key": "<AWS-SECRET-ACCESS-KEY>"
    }
  ]
}
```

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
92405792	Failed to regenerate access-key and secret-key for user.
92406082	Cannot perform "regenerate_keys" and "delete_keys" operations simultaneously on an S3 user.
92406081	The "regenerate_keys" operation on S3 User "user-2" in SVM "vs1" succeeded. However, modifying all of the other S3 user properties failed. Reason: resource limit exceeded. Retry the operation again without specifying the "regenerate_keys" parameter.
92406080	Cannot delete root user keys because there exists at least one S3 SnapMirror relationship that is using these keys.
92406083	The maximum supported value for user key expiry configuration is "1095" days.
92406088	The "key_time_to_live" parameter can only be used when the "regenerate_keys" operation is performed.
92406096	The user does not have permission to access the requested resource \"{0}\".
92406097	Internal error. The operation configuration is not correct.

Error Code	Description
92406196	The specified value for the "key_time_to_live" field cannot be greater than the maximum limit specified for the "max_key_time_to_live" field in the object store server.

| 92406197 | Object store user "user-2" must have a non-zero value for the "key_time_to_live" field because the maximum limit specified for the "max_key_time_to_live" field in the object store server is not zero. |
92406200 | An object store user with the same access-key already exists. | | 92406201 | Missing access-key or secret-key. Either provide both of the keys or none. If not provided, keys are generated automatically. | |
92406202 | The "delete_keys" operation must be performed without specifying the user keys. | | 92406205 |
The object store user access key contains invalid characters. Valid characters are 0-9 and A-Z. | | 92406308 |
Cannot disable user "user1" in SVM "vs1" because the user belongs to at least one object store group.
Remove the user from all groups before disabling the user. |

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

s3_user

This is a container of S3 users.

Name	Type	Description
access_key	string	Specifies the access key for the user.
comment	string	Can contain any additional information about the user being created or modified.
key_expiry_time	string	Specifies the date and time after which keys expire and are no longer valid.

Name	Type	Description
key_time_to_live	string	<p>Indicates the time period from when this parameter is specified:</p> <ul style="list-style-type: none"> • when creating or modifying a user or • when the user keys were last regenerated, after which the user keys expire and are no longer valid. • Valid format is: 'PnDTnHnMnS PnW'. For example, P2DT6H3M10S specifies a time period of 2 days, 6 hours, 3 minutes, and 10 seconds. • If the value specified is '0' seconds, then the keys won't expire.
secret_key	string	Specifies the secret key for the user.
svm	svm	SVM, applies only to SVM-scoped objects.

collection_links

s3_service_user_post_response

Name	Type	Description
access_key	string	Specifies the access key for the user.
key_expiry_time	string	Specifies the date and time after which the keys expire and are no longer valid.
name	string	The name of the user.
secret_key	string	Specifies the secret key for the user.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.